(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 4 120 167 A1

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
18.01.2023 Bulletin 2023/03

(21) Application number: **21857394.7**

(22) Date of filing: **07.07.2021**

(51) International Patent Classification (IPC):
G06Q 20/38 *(2012.01)*

(52) Cooperative Patent Classification (CPC):
G06Q 20/38

(86) International application number:
PCT/CN2021/104999

(87) International publication number:
WO 2022/037299 (24.02.2022 Gazette 2022/08)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **20.08.2020 CN 202010840924**

(71) Applicant: **Tencent Technology (Shenzhen) Company Limited**
Shenzhen, Guangdong 518057 (CN)

(72) Inventors:
- **CHENG, Zhehao**
  Shenzhen, Guangdong 518057 (CN)
- **DONG, Jingran**
  Shenzhen, Guangdong 518057 (CN)
- **CHEN, Shouzhi**
  Shenzhen, Guangdong 518057 (CN)

(74) Representative: **EP&C**
P.O. Box 3241
2280 GE Rijswijk (NL)

(54) ABNORMAL BEHAVIOR DETECTION METHOD AND APPARATUS, AND ELECTRONIC DEVICE AND COMPUTER-READABLE STORAGE MEDIUM

(57) This application provides an abnormal behavior detection method and apparatus, an electronic device, and a computer-readable storage medium. The method includes: obtaining a first target sub-model corresponding to a first target object from a first preset object model; determining an abnormal data volume from the first target sub-model based on a preset model parameter, and determining a first detection result corresponding to to-be-detected behavior information based on a comparison result between a target data volume and the abnormal data volume; obtaining a second target sub-model corresponding to a second target object and having a highest similarity with the first target sub-model from a second preset object model; obtaining a target maximum data volume corresponding to the second target sub-model, and determining a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume; and determining a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result.

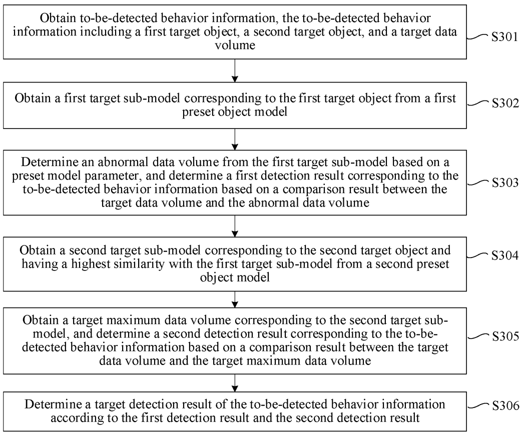

Obtain to-be-detected behavior information, the to-be-detected behavior information including a first target object, a second target object, and a target data volume
S301
Obtain a first target sub-model corresponding to the first target object from a first preset object model
S302
Determine an abnormal data volume from the first target sub-model based on a preset model parameter, and determine a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume
S303
Obtain a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model
S304
Obtain a target maximum data volume corresponding to the second target sub-model, and determine a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume
S305
Determine a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result
S306

FIG. 3

Processed by Luminess, 75001 PARIS (FR)

Description

RELATED APPLICATION

[0001] This application claims priority to Chinese Patent Application No. 202010840924.8, filed with the China National Intellectual Property Administration on August 20, 2020, which is incorporated herein by reference in its entirety.

FIELD OF THE TECHNOLOGY

[0002] This application relates to information processing technologies in the field of computer application, and in particular, to an abnormal behavior detection method and apparatus, an electronic device, and a computer-readable storage medium.

BACKGROUND OF THE APPLICATION

[0003] With the rapid development of the computer application technologies, an application with various network functions is more widely applied. However, during application of the network functions, malicious processing such as false brushing or stolen account payment is often performed in an abnormal manner. In view of this, to improve the network security, abnormal behavior detection has become increasingly important.

[0004] Generally, abnormal behavior detection is usually performed in an unsupervised manner. For example, historical behavior information is clustered to obtain a plurality of clusters, and after to-be-detected behavior information is obtained, the abnormality of the to-be-detected behavior information is determined by judging an ownership relationship between the to-be-detected behavior information and the plurality of clusters. However, during the abnormal behavior detection, since a feature dimension of the to-be-detected behavior information is low, in a case that clustering processing is performed based on the low-dimensional feature to determine a detection result, an error is probably existed in the detection result, resulting in a relatively low accuracy of the abnormal behavior detection.

SUMMARY

[0005] Embodiments of this application provide an abnormal behavior detection method and apparatus, an electronic device, and a computer-readable storage medium, to improve the accuracy of abnormal behavior detection.

[0006] Technical solutions in the embodiments of this application are implemented as follows:

[0007] An embodiment of this application provides an abnormal behavior detection method, performed by an electronic device, the method including:

obtaining to-be-detected behavior information, the to-be-detected behavior information including a first target object, a second target object, and a target data volume;

obtaining a first target sub-model corresponding to the first target object from a first preset object model;

determining an abnormal data volume from the first target sub-model based on a preset model parameter, and determining a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume;

obtaining a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model;

obtaining a target maximum data volume corresponding to the second target sub-model, and determining a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume; and

determining a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result.

[0008] An embodiment of this application provides an abnormal behavior detection apparatus, including:

an information obtaining module, configured to obtain to-be-detected behavior information, the to-be-detected behavior information including a first target object, a second target object, and a target data volume;

a first detection module, configured to obtain a first target sub-model corresponding to the first target object from a first preset object model,

the first detection module being further configured to determine an abnormal data volume from the first target sub-model based on a preset model parameter, and determine a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume;

a second detection module, configured to obtain a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model,

the second detection module being further configured to obtain a target maximum data volume corresponding to the second target sub-model, and determine a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume; and

a result determination module, configured to determine a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result.

[0009] An embodiment of this application provides an electronic device for abnormal behavior detection, including

a memory, configured to store executable instructions; and

a processor, configured to implement, when executing the executable instructions stored in the memory, the abnormal behavior detection method provided in this embodiment of this application.

[0010] An embodiment of this application provides a computer-readable storage medium, storing executable instructions, the executable instructions, when executed by a processor, causing the processor to implement the abnormal behavior detection method provided in this embodiment of this application.

[0011] The embodiments of this application have at least the following beneficial effects: In a case that the to-be-detected behavior information includes three dimensional features of the first target object, the second target object, and the target data volume, when the target detection result of whether the to-be-detected behavior information is abnormal is determined according to results of respectively comparing the target data volume with the abnormal data volume and the target maximum data volume, since the abnormal data volume is an abnormality judgment condition for the first target object determined based on the first preset object model, and the target maximum data volume is an abnormality judgment condition for the second target object determined based on the second preset object model, in a low-dimensional feature, whether the target data volume is within a preset interval is determined from two dimensions of the first target object and the second target object, to further accurately obtain the target detection result of whether the to-be-detected behavior information is abnormal, thereby improving the accuracy of abnormal behavior detection.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012]

FIG. 1 is an optional schematic architecture diagram of an abnormal behavior detection system according to an embodiment of this application.

FIG. 2 is a schematic diagram of a composition structure of a server in FIG. 1 according to an embodiment of this application.

FIG. 3 is an optional schematic flowchart of an abnormal behavior detection method according to an embodiment of this application.

FIG. 4 is an exemplary schematic diagram of determining an abnormal data volume according to an embodiment of this application.

FIG. 5 is another optional schematic flowchart of an abnormal behavior detection method according to an embodiment of this application.

FIG. 6a is an exemplary schematic diagram of a to-be-converted data volume according to an embodiment of this application.

FIG. 6b is an exemplary schematic diagram of data volume conversion according to an embodiment of this application.

FIG. 7 is an exemplary schematic diagram of obtaining a similarity according to an embodiment of this application.

FIG. 8 is an exemplary schematic diagram of obtaining a merged sub-model according to an embodiment of this application.

FIG. 9 is an exemplary schematic flowchart of abnormal behavior detection according to an embodiment of this application.

FIG. 10 is an exemplary schematic diagram of obtaining a model according to an embodiment of this application.

FIG. 11 is an exemplary schematic diagram of a model according to an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

[0013] To make the objectives, technical solutions, and advantages of this application clearer, the following describes this application in further detail with reference to the accompanying drawings. The described embodiments are not to be considered as a limitation to this application. All other embodiments obtained by a person of ordinary skill in the art without creative efforts shall fall within the protection scope of this application.

[0014] In the following descriptions, related "some embodiments" describe a subset of all possible embodiments. However, it may be understood that the "some embodiments" may be the same subset or different subsets of all the possible embodiments, and may be combined with each other without conflict.

[0015] In the following descriptions, the included term "first/second" is merely intended to distinguish similar objects but does not necessarily indicate a specific order of an object. It may be understood that "first/second" is interchangeable in terms of a specific order or sequence if permitted, so that the embodiments of this application described herein can be implemented in a sequence in addition to the sequence shown or described herein.

[0016] Unless otherwise defined, meanings of all technical and scientific terms used in the embodiments of this application are the same as those usually understood by a person skilled in the art to which this application belongs. Terms used in the embodiments of this application are merely intended to describe objectives of the embodiments of this application, but are not intended to limit this application.

[0017] Before the embodiments of this application are further described in detail, a description is made on nouns and terms in the embodiments of this application, and the nouns and terms in the embodiments of this application are applicable to the following explanations.

1) Abnormal behavior detection: It refers to detection of whether data corresponding to a user’s operation behavior conforms to a preset operation process or an actual process, for example, detection of stolen account payment and false brushing.

2) Offline environment: It refers to a platform for processing massive f data (for example, billion-level data) based on a data mining tool (for example, "hadoop" and "spark"). Usually there is a relatively high delay (for example, a delay of one day), causing poor real-time performance.

3) Real-time/online environment: It is used for a platform for efficiently storing and computing to-be-processed data in real time, a delay is usually within milliseconds, the complexity is low, and the real-time performance is relatively high.

[0018] Generally, abnormal behavior detection is usually implemented in an unsupervised and supervised manner. In a case that abnormal behavior detection is performed in an unsupervised manner, it indicates that an unsupervised algorithm is applied to the abnormal behavior detection. For example, in a case that behavior information in an application scenario obeys mixture Gaussian distribution, during abnormal behavior detection, whether to-be-detected behavior information is abnormal may be determined by judging whether the to-be-detected behavior information obeys mixture Gaussian distribution. In another example, historical behavior information is clustered to obtain a plurality of clusters, and after to-be-detected behavior information is obtained, the abnormality of the to-be-detected behavior information is determined by judging an ownership relationship between the to-be-detected behavior information and the plurality of clusters. In still another example, behavioral information corresponding to an isolated point in a space is determined as abnormal behavioral information by using an outlier detection algorithm (for example, an isolation forest algorithm). However, when abnormal behavior detection is performed in an unsupervised manner, the feature is low-dimensional in a case that the to-be-detected behavior information includes three dimensional features of a first target object, a second target object, and a target data volume (for example, a user, a merchant, and an amount; a user, a product, and an amount; or a user, an article, and views); and when detection is performed based on the low-dimensional feature in an unsupervised manner to determine a detection result, an error is probably existed in the detection result, resulting in a relatively low accuracy of the abnormal behavior detection. In addition, in a case that a feature of more than three dimensions is obtained for unsupervised detection, a detection duration is relatively long due to a relatively high feature dimension/complexity, resulting in poor real-time performance of the detection.

[0019] In a case that abnormal behavior detection is performed in a supervised manner, it indicates that a sample is labeled, a network model is trained by using a sample feature and labeled information, and then whether the to-be-detected behavior information is abnormal is detected by using the network model. However, when abnormal behavior is performed in a supervised manner, the sample needs to be labeled, and it is less feasible to perform labeling in a case that a data volume of the sample is relatively large, for example, reaches a level of hundred million. For example, in a case that whether payment is abnormal is detected, since hundreds of millions of payments are generated every day, it is less feasible to perform manual labeling. In addition, a long labeling duration may result in a relatively long duration for network model training. After the network model is trained, the trained network model may no longer be applicable to the current application scenario in a case that the behavior information in the application scenario changes rapidly and abnormal behavior detection in the application scenario is time-based. As a result, labeling is less feasible and cannot be applied to an application scenario with higher timeliness.

[0020] In view of this, embodiments of this application provide an abnormal behavior detection method and apparatus, an electronic device, and a computer-readable storage medium, which can quickly and accurately perform abnormal behavior detection and is applicable to an application scenario with higher timeliness.

[0021] The following describes an exemplary application of an electronic device for abnormal behavior detection (hereinafter briefly referred to as an abnormal behavior detection device) provided in the embodiments of this application. The abnormal behavior detection device provided in the embodiments of this application may be implemented as various types of terminals such as a notebook computer, a tablet computer, a desktop computer, a set top box, or a mobile device (such as a mobile phone, a portable music player, a personal digital assistant, a dedicated messaging device, a portable game device, an in-vehicle device, a smartphone, or a smart watch), or may be implemented as a server. An exemplary application in which the device is implemented as a server is described below.

[0022] Referring to FIG. 1, FIG. 1 is an optional schematic architecture diagram of an abnormal behavior detection system according to an embodiment of this application. As shown in FIG. 1, to support an abnormal behavior detection application, in an abnormal behavior detection system 100, terminals 200 (where a terminal 200-1 and a terminal 200-2 are shown as an example) are connected to a server 400 (the abnormal behavior detection device) through a network 300. The network 300 may be a wide area network, a local area network, or a combination of thereof. In addition, the abnormal behavior detection system 100 further includes a database 500.

[0023] The database 500 is configured to store a first preset object model and a second preset object model, and provide the first preset object model and the second preset object model to the server 400, to implement abnormal behavior detection.

[0024] The terminal 200-1 is configured to receive a payment operation by a user through a control 200-111 (a payment button is exemplarily shown) on a graphical interface 200-11, send, in response to the payment operation, to-be-detected behavior information including a merchant (a first target object), a user (a second target object), and an amount (a target data volume) to the server 400 through the network 300, receive, through the network 300, a target detection result sent by the server 400, and display the target detection result on a graphical interface 200-12.

[0025] The terminal 200-2 is configured to receive a reading operation by the user through a control 200-211 (a reading button is exemplarily shown) on a graphical interface 200-21, send, in response to the reading operation, to-be-detected behavior information including an article (a first target object), a user (a second target object), and views (a target data volume) to the server 400 through the network 300, receive, through the network 300, a target detection result sent by the server 400, and display the target detection result on a graphical interface 200-22.

[0026] The server 400 is configured to: obtain to-be-detected behavior information from the terminals 200 through the network 300, the to-be-detected behavior information including a first target object, a second target object, and a target data volume; obtain a first target sub-model corresponding to the first target object from a first preset object model provide by the database 500; determine an abnormal data volume from the first target sub-model based on a preset model parameter, and determine a first detection result corresponding to the to-be-detected behavior information by comparing the target data volume with the abnormal data volume; obtain a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model provided by the database 500; obtain a target maximum data volume corresponding to the second target sub-model, and determine a second detection result corresponding to the to-be-detected behavior information by comparing the target data volume with the target maximum data volume; determine a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result; and send the target detection result to the terminals 200 through the network 300.

[0027] In some embodiments, the server 400 may be an independent physical server, or may be a server cluster or a distributed system formed by a plurality of physical servers, or may be a cloud server that provides basic cloud computing services such as a cloud service, a cloud database, cloud computing, a cloud function, cloud storage, a network service, cloud communication, a middleware service, a domain name service, a security service, a content delivery network (CDN), big data, and an artificial intelligence platform. The terminal and the server may be directly or indirectly connected in a wired or wireless communication manner. This is not limited in the embodiments of the present disclosure.

[0028] Referring to FIG. 2, FIG. 2 is a schematic diagram of a composition structure of a server in FIG. 1 according to an embodiment of this application. The server 400 shown in FIG. 2 includes at least one processor 410, a memory 450, at least one network interface 420, and a user interface 430. Components in the server 400 are coupled together by using a bus system 440. It may be understood that the bus system 440 is configured to implement connection and communication between the components. In addition to a data bus, the bus system 440 further includes a power bus, a control bus, and a status signal bus. However, for ease of clear description, all types of buses are marked as the bus system 440 in FIG. 2.

[0029] The processor 410 may be an integrated circuit chip having a signal processing capability, for example, a general purpose processor, a digital signal processor (DSP), or another programmable logic device (PLD), discrete gate, transistor logical device, or discrete hardware component. The general purpose processor may be a microprocessor, any conventional processor, or the like.

[0030] The user interface 430 includes one or more output apparatuses 431 that enable presentation of media content, including one or more speakers and/or one or more visualization displays. The user interface 430 further includes one or more input apparatuses 432, including user interface components helping a user input, such as a keyboard, a mouse, a microphone, a touch display screen, a camera, and other input buttons and controls.

[0031] The memory 450 may be a removable memory, a non-removable memory, or a combination thereof. Exemplary hardware devices include a solid-state memory, a hard disk drive, an optical disc driver, or the like. The memory 450 optionally includes one or more storage devices physically away from the processor 410.

[0032] The memory 450 includes a volatile memory or a non-volatile memory, or may include both a volatile memory and a non-volatile memory. The non-volatile memory may be a read-only memory (ROM), and the volatile memory may be a random access memory (RAM). The memory 450 described in this embodiment of this application includes any suitable type of memory.

[0033] In some embodiments, the memory 450 may store data to support various operations. Examples of the data include programs, modules, and data structures, or a subset or a superset thereof. The descriptions are made below by using examples.

[0034] An operating system 451 includes a system program configured to process various basic system services and perform a hardware-related task, for example, a framework layer, a core library layer, and a driver layer, and is configured to implement various basic services and process a hardware-related task.

[0035] A network communication module 452 is configured to reach another computing device through one or more (wired or wireless) network interfaces 420. Exemplary network interfaces 420 include: Bluetooth, wireless compatible authentication (Wi-Fi), a universal serial bus (USB), and the like.

[0036] A display module 453 is configured to display information by using an output apparatus 431 (for example, a display screen or a speaker) associated with one or more user interfaces 430 (for example, a user interface configured to operate a peripheral device and display content and information).

[0037] An input processing module 454 is configured to detect one or more user inputs or interactions from one of the one or more input apparatuses 432 and translate the detected input or interaction.

[0038] In some embodiments, the abnormal behavior detection apparatus provided in this embodiment of this application may be implemented in a form of software. FIG. 2 shows an abnormal behavior detection apparatus 455 stored in the memory 450, which may be software in a form such as a program and a plug-in, and includes the following software modules: an information obtaining module 4551, a first detection module 4552, a second detection module 4553, a result determination module 4554, and a model obtaining module 4555. Such modules are logical, and therefore may be randomly combined or further divided according to a function to be implemented. A function of each module is described below.

[0039] In some other embodiments, the abnormal behavior detection apparatus provided in this embodiment of this application may be implemented by using hardware. For example, the abnormal behavior detection apparatus provided in this embodiment of this application may be a processor in a form of a hardware decoding processor, programmed to perform the abnormal behavior detection method provided in the embodiments of this application. For example, the processor in the form of a hardware decoding processor may use one or more application-specific integrated circuits (ASIC), a DSP, a programmable logic device (PLD), a complex programmable logic device (CPLD), a field-programmable gate array (FPGA), or other electronic components.

[0040] The abnormal behavior detection method provided in the embodiments of this application is described below with reference to an exemplary application in which the abnormal behavior detection device provided in this embodiment of this application is implemented as a server.

[0041] Referring to FIG. 3, FIG. 3 is an optional schematic flowchart of an abnormal behavior detection method according to an embodiment of this application, and the method is described with reference to steps shown in FIG. 3.

[0042] S301: Acquire to-be-detected behavior information, the to-be-detected behavior information including a first target object, a second target object, and a target data volume.

[0043] In this embodiment of this application, in a case that the user performs an operation on a functional application in a terminal, for example, performing payment, reading an article, or clicking on an advertisement, the terminal generates operation data in response to the operation performed by the user, and sends the operation data to the server, and then the server receives the to-be-detected behavior information. In this way, the to-be-detected behavior information is obtained.

[0044] The to-be-detected behavior information is a detection object, including a first target object, a second target object, and a target data volume. The first target object is an operated object, for example, an advertisement, a merchant, a product, or an article. The second target object is an operation object, for example, a user, or the like. The target data volume is a data volume generated by performing an operation on the first target object by the second target object, for example, an amount, clicks, or views.

[0045] S302: Obtain a first target sub-model corresponding to the first target object from a first preset object model.

[0046] In this embodiment of this application, the server pre-stores the first preset object model, or the server can obtain the first preset object model in advance. The first preset object model is a model corresponding to each first object, and the model is data volume distribution information. Since the first target object is a first object, the server can obtain a model corresponding to the first target object from the first preset object model. In this case, the first target sub-model is obtained.

[0047] In other words, the first preset object model is a correspondence between first objects and the data volume distribution information. Since the first target object is a first object, on the basis of the correspondence between the first objects and the data volume distribution information, the server matches the first target object with each first object in the correspondence between the first objects and the data volume distribution information, to obtain a first object from the first objects through matching, and determines data volume distribution information corresponding to the matched first object as the first target sub-model.

[0048] The first target sub-model is data volume distribution information corresponding to the first target object, for example, a histogram of an amount corresponding to a merchant A, or distribution of views corresponding to an article B.

[0049] In addition, in this embodiment of this application, in a case that the model corresponding to the first target object is not obtained from the first preset object model, the server constructs a first target sub-model for the first target object, and adds the first target sub-model corresponding to the first target object to the first preset object model.

[0050] S303: Determine an abnormal data volume from the first target sub-model based on a preset model parameter, and determine a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume.

[0051] In this embodiment of this application, the server stores the preset model parameter, or the server can obtain the preset model parameter in advance. The preset model parameter is a preset quantile in the data volume distribution information, and is used for determining a preset range of a data volume corresponding to the first target object. The determined preset interval of the data volume corresponding to the first target object is an abnormality judgment condition corresponding to the first target object. Therefore, the server can determine a target position corresponding to the preset model parameter from the first target sub-model, where a data volume of the target position is the abnormal data volume. Next, after comparing the target data volume with the abnormal data volume, the server can determine whether the target data volume is within the preset interval (ranging from zero to the abnormal data volume) of the data volume corresponding to the first target object according to the comparison result between the target data volume and the abnormal data volume. In this case, the first detection result corresponding to the to-be-detected behavior information is obtained.

[0052] The first detection result is a result of whether the to-be-detected behavior information is abnormal determined for the first target object. In a case that the target data volume is greater than the abnormal data volume, it indicates that the target data volume exceeds the preset interval of the data volume corresponding to the first target object, and the server determines the first detection result that the to-be-detected behavior information is abnormal with respect to the first target object. In a case that the target data volume is less than or equal to the abnormal data volume, it indicates that the target data volume is within the preset interval of the data volume corresponding to the first target object, and the server determines the first detection result that the to-be-detected behavior information is normal with respect to the first target object.

[0053] Exemplarily, referring to FIG. 4, FIG. 4 is an exemplary schematic diagram of determining an abnormal data volume according to an embodiment of this application. As shown in FIG. 4, in a histogram 4-1 (the first target sub-model), a transverse axis is an amount value, and a longitudinal axis is a probability value. Probability values of amount segments in the histogram 4-1 are superimposed in ascending order of the amount value in a case that the preset model parameter is the 99th quantile, and in a case that a superposition result is greater than 99%, an amount value corresponding to a position 14-2 (which is a target position, a probability of an amount less than an amount value corresponding to the position 14-2 is greater than 99%) is the abnormal data volume.

[0054] S304: Obtain a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model.

[0055] In this embodiment of this application, the server pre-stores the second preset object model, or the server can obtain the second preset object model in advance. The second preset object model is a model set formed by each piece of data volume distribution information corresponding to the second object with respect to each first object. Since the second target object is a second object, the server can obtain a model group corresponding to the second target object from the second preset object model, and match a model having a highest similarity with the first target sub-model from the obtained model group corresponding to the second target object, so that the second target sub-model is obtained.

[0056] In other words, in the second preset object model, the server matches each second target object with the second objects to obtain matched each piece of data volume distribution information (the model group) corresponding to the second object with respect to the each first object, and further obtains data volume distribution information most similar to the obtained first target sub-model from the each piece of data volume distribution information, where the data volume distribution information most similar to the first target sub-model is the second target sub-model. Data volume distribution information corresponding to the each first object in the first preset object model is different from data volume distribution information corresponding to the each first object in the second preset object model, the data volume distribution information corresponding to the each first object in the second preset object model is obtained by processing the data volume distribution information corresponding to the each first object in the first preset object model, which is data volume distribution information corresponding to the second object with respect to the first object.

[0057] The second target sub-model is data volume distribution information corresponding to the second target object with respect to the first target object, for example, an amount histogram of a user C with respect to the merchant A, or distribution of views of a user D with respect to the article B.

[0058] S305: Obtain a target maximum data volume corresponding to the second target sub-model, and determine a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume.

[0059] In this embodiment of this application, after the server obtains the second target sub-model, since the second preset object model not only includes a model group corresponding to each second object, but also includes a maximum data volume corresponding to the each second object, the server determines the target maximum data volume based on a maximum data volume corresponding to the second target object in the second preset object model. In other words, the target maximum data volume may be the maximum data volume corresponding to the second target object, or may be determined based on the maximum data volume corresponding to the second target object in the second preset object model. This is not specifically limited in this embodiment of this application.

[0060] In this case, the server obtains the target maximum data volume, so that a preset interval of a data volume corresponding to the second target object is determined, where the determined preset interval of the data volume corresponding to the second target object is an abnormality judgment condition corresponding to the second target object. Therefore, after comparing the target data volume with the target maximum data volume, the server can determine whether the target data volume is within the preset interval (ranging from zero to the target maximum data volume) of the data volume corresponding to the second target object according to the comparison result between the target data volume and the target maximum data volume. In this case, the second detection result corresponding to the to-be-detected behavior information is obtained.

[0061] The second detection result is a result of whether the to-be-detected behavior information is abnormal determined for the second target object. In a case that the target data volume is greater than the target maximum data volume, it indicates that the target data volume exceeds the preset interval of the data volume corresponding to the second target object, and the server determines the second detection result that the to-be-detected behavior information is abnormal with respect to the second target object. In a case that the target data volume is less than or equal to the target maximum data volume, it indicates that the target data volume is within the preset interval of the data volume corresponding to the second target object, and the server determines the second detection result that the to-be-detected behavior information is normal with respect to the second target object.

[0062] S306: Determine a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result.

[0063] In this embodiment of this application, after obtaining the first detection result and the second detection result, the server determines the target detection result of the to-be-detected behavior information according to the first detection result and the second detection result. The target detection result indicates whether the to-be-detected behavior information is abnormal.

[0064] The determining, by the server, a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result includes: in a case that the first detection result is that the to-be-detected behavior information is abnormal with respect to the first target object and the second detection result is that the to-be-detected behavior information is abnormal with respect to the second target object, determining, by the server, the target detection result including that the to-be-detected behavior information is abnormal; in a case that the first detection result is that the to-be-detected behavior information is normal with respect to the first target object and the second detection result is that the to-be-detected behavior information is abnormal with respect to the second target object, determining, by the server, the target detection result including that the to-be-detected behavior information is abnormal, determining the target detection result including that the to-be-detected behavior information is normal, and determining the to-be-detected behavior information as to-be-audited behavior information, to further detect by performing intelligent detection processing in manual manner; in a case that the first detection result is that the to-be-detected behavior information is normal with respect to the first target object and the second detection result is that the to-be-detected behavior information is normal with respect to the second target object, determining, by the server, the target detection result including that the to-be-detected behavior information is normal; and in a case that the first detection result is that the to-be-detected behavior information is abnormal with respect to the first target object and the second detection result is that the to-be-detected behavior information is normal with respect to the second target object, determining, by the server, the target detection result including that the to-be-detected behavior information is normal, determining the target detection result including that the to-be-detected behavior information is abnormal, and determining the to-be-detected behavior information as to-be-audited behavior information, to further detect by performing intelligent detection processing in manual manner.

[0065] In this embodiment of this application, after obtaining the target detection result, the server may further determine target processing information according to the target detection result. The target processing information is a processing manner for the to-be-detected behavior information, for example, when the to-be-detected behavior information is the payment operation, in a case that the target detection result is that the to-be-detected behavior information is abnormal, the target processing information is the processing of blocking the payment operation. In another example, when the to-be-detected behavior information is advertisement clicking, in a case that the target detection result is that the to-be-detected behavior information is abnormal, the target processing information is the processing of blocking the advertisement clicking.

[0066] It may be understood that, in a case that the to-be-detected behavior information includes three dimensional features of the first target object, the second target object, and the target data volume, when the target detection result of whether the to-be-detected behavior information is abnormal is determined according to results of respectively comparing the target data volume with the abnormal data volume and the target maximum data volume, since the abnormal data volume is an abnormality judgment condition for the first target object determined based on the first preset object model, and the target maximum data volume is an abnormality judgment condition for the second target object determined based on the second preset object model, in a low-dimensional feature, whether the target data volume is within a preset interval is determined from two dimensions of the first target object and the second target object, to further accurately obtain the target detection result of whether the to-be-detected behavior information is abnormal, so that the accuracy of abnormal behavior detection is relatively high.

[0067] Referring to FIG. 5, FIG. 5 is another optional schematic flowchart of an abnormal behavior detection method according to an embodiment of this application. As shown in FIG. 5, in this embodiment of this application, before S302, the method further includes S307 to S311. In other words, before the obtaining, by the server, a first target sub-model corresponding to the first target object from a first preset object model, the abnormal behavior detection method further includes S307 to S311. The steps are described as follows:

[0068] S307: Obtain a behavior information sample.

[0069] In this embodiment of this application, the server obtains behavior information in a current cycle, so that the behavior information sample is obtained, for example, payment orders in a last week, or reading records in a last month. The current cycle refers to the most recent preset cycle.

[0070] The behavior information sample is a set formed by behavior information corresponding to a first object, a second object, and a data volume in a current cycle, and therefore, each piece of behavior information in the behavior information sample includes the first object, the second object, and the data volume.

[0071] S308: Aggregate the behavior information sample according to a first preset object type to obtain a data volume set corresponding to each first object, construct a first sub-model corresponding to the each first object according to the data volume set, and determine each constructed first sub-model corresponding to the each first object as the first preset object model.

[0072] After obtaining the behavior information sample, the server aggregates the behavior information sample according to different preset types, to obtain the first preset object model and the second preset object model. The different preset types include a first preset object type (for example, a merchant type or a product type) and a second preset object type (for example, a user), where the first preset object type is an object type to which the first object belongs, and the second preset object type is an object type to which the second object belongs. Therefore, the data volume set corresponding to the each first object is obtained in a case that the server aggregates the behavior information sample according to the first preset object type, to obtain each data volume corresponding to each first object.

[0073] The object type corresponding to each first object is the first preset object type. The data volume set is a set formed by a data volume of the each first object with respect to the second object.

[0074] In this embodiment of this application, after obtaining the data volume set, the server determines data volume distribution information corresponding to each first object according to the data volume set, so that the first sub-model corresponding to the each first object is constructed. The first sub-model corresponding to the each first object is obtained after the first sub-model corresponding to the each first object is constructed, where the first sub-model corresponding to the each first object is the first preset object model. The each first object refers to any object in the first objects, and the first preset object model refers to a set formed by the first sub-model of the each first object. The first target sub-model is a first sub-model.

[0075] S309: Aggregate the behavior information sample according to a second preset object type, to obtain a first object set and a maximum data volume corresponding to each second object.

[0076] In this embodiment of this application, the first object set corresponding to the each second object is obtained in a case that the server aggregates the behavior information sample according to the second preset object type, to obtain the first object corresponding to the each second object. Each data volume corresponding to the each second object is further obtained in a case that the server aggregates the behavior information sample according to the second preset object type, and a maximum data volume is selected from the each data volume corresponding to the each second object, so that the maximum data volume corresponding to the each second object.

[0077] S310: Traverse the first object set, and construct at least one second object sub-model based on the first sub-model corresponding to the traversed first object.

[0078] In this embodiment of this application, after obtaining the first object set, the server traverses the first objects in the first object set, and the traversed first objects is matched with the first objects in the first preset object model, where a model corresponding to a matched first object is a first sub-model corresponding to the traversed first object. The server constructs the at least one second object sub-model corresponding to the each second object by using the first sub-model corresponding to the traversed first object.

[0079] The at least one second object sub-model is a set formed by the data volume of the first object associated with the each second object, for example, an amount histogram of a user C with respect to the merchant A, an amount histogram of the user C with respect to a merchant E, and an amount histogram of the user C with respect to a merchant F. The traversed first object is any first object in the first object set.

[0080] S311: Combine the at least one second object sub-model and the maximum data volume into a second sub-model corresponding to the each second object, and determine each combined second sub-model corresponding to the each second object as the second preset object model.

[0081] After obtaining the at least one second object sub-model corresponding to the each second object, the server combines the at least one second object sub-model and the maximum data volume, where an obtained combination result is the second sub-model corresponding to the each second object. The second preset object model of the each second sub-model corresponding to the each second object is obtained in a case that the second sub-model corresponding to the each second object is obtained. The each second object refers to any object in the second objects, and the second preset object model refers to a set formed by the second sub-model of the each second object.

[0082] In this embodiment of this application, the constructing, by the server, a first sub-model corresponding to the each first object according to the data volume set described in S308 includes S3081 to S3085. The steps are described as follows:

S3081: Obtain a data volume range corresponding to each data volume in the data volume set.

[0083] In this embodiment of this application, the server extracts a minimum data volume and a maximum data volume from each data volume in the data volume set, where a range between the minimum data volume and the maximum data volume is the data volume range.

[0084] S3082: Segment the data volume range to obtain a plurality of target segments.

[0085] In this embodiment of this application, the server segments the data volume range according to a magnitude or quantity of a preset segment, so that the plurality of target segments are obtained.

[0086] S3083: Collect statistics on a target quantity of data volumes of each target segment in the plurality of target segments from the data volume set.

[0087] In this embodiment of this application, after obtaining the plurality of target segments and the data volume set, the server determines a target segment to which the each data volume in the data volume set belongs, to further collect statistics a quantity of the data volumes of the each target segment in the plurality of target segments. The quantity of the data volumes of the each target segment obtained by collecting statistics is the target quantity corresponding to the each target segment.

[0088] S3084: Determine a ratio of the target quantity to a set element quantity corresponding to the data volume set as a probability value corresponding to the each target segment.

[0089] In this embodiment of this application, the server collects statistics on the quantity of the data volumes in the data volume set, the quantity of the data volumes in the data volume set obtained by collecting statistics is the set element quantity corresponding to the data volume set. In this case, a ratio is calculated by using the target data volume as a numerator and using the set element quantity as a denominator, and an obtained ratio result is the probability value corresponding to the each target segment. The plurality of probability values corresponding to the plurality of target segments are obtained after the probability value corresponding to the each target segment is obtained, where the plurality of target segments and the plurality of probability values are in a one-to-one correspondence.

[0090] S3085: Determine a plurality of determined probability values corresponding to the plurality of target segments as the first sub-model corresponding to the each first object.

[0091] The first sub-model is the plurality of probability values corresponding to the plurality of target segments associated with the first objects.

[0092] In this embodiment of this application, S3081 may be implemented through S30811 and S30812. In other words, the obtaining, by the server, a data volume range corresponding to each data volume in the data volume set includes S30811 and S30812. The steps are described as follows:

[0093] S30811: Convert the each data volume in the data volume set, to obtain a converted data volume set.

[0094] Since distribution corresponding to the each data volume in the data volume set is usually logarithmic normal distribution, there is a smooth portion (a long tail portion) in the logarithmic normal distribution, a probability corresponding to the smooth portion is close to 0, a detection result for a larger data volume is inaccurate, and data support cannot be provided for subsequent abnormal behavior detection. Therefore, to improve the accuracy of abnormal behavior detection, the server converts the each data volume in the data volume set and eliminates the smooth portion, so that distribution corresponding to each converted data volume in a data volume set after conversion obeys standard normal distribution.

[0095] The conversion herein may be a logarithmic conversion, or may be a simultaneous reduction of a preset multiple, or may be a corresponding multiplication performed on the each data volume by using different weights, or the like. This is not specifically limited in this embodiment of this application. The data volume is converted in a process of model obtaining, the data volume described in the processes of model obtaining and model application is a data volume after conversion.

[0096] Referring to FIG. 6a, in a case that the data volume is an amount value, since an amount value corresponding to micropayment is sometimes small, for example, several yuan, and an amount value corresponding to large payment is sometimes large, for example, hundreds of thousands of yuan, a smooth portion 6-11 may appear in a distribution curve 6-1 corresponding to the data volume, a probability in probability distribution corresponding to the smooth portion 6-11 is almost 0, and data support cannot be provided for subsequent abnormal payment detection. In FIG. 6a, a transverse axis is an amount value, and a longitudinal axis is a probability value. In this case, the data volume is converted by using a natural logarithm (In), and the distribution curve 6-1 in FIG. 6a is converted into a distribution curve 6-2 in FIG. 6b. In FIG. 6b, a transverse axis is a converted amount value, and a longitudinal axis is a probability value. It is easy to learn that, logarithm-taking operation is performed on the amount value, so that a fluctuation of several yuan can be encoded by the model during the micropayment, and a fluctuation of thousands or even tens of thousands of yuan can be encoded by the model during the large payment. Such a small sensitive and large insensitive trend is consistent with a change curve of a logarithmic function, for example, In 2 - In 1 ≅ In 20000 - In 10000.

[0097] S30812: Determine a range corresponding to each converted data volume in the converted data volume set as the data volume range.

[0098] After obtaining the converted data volume set, the server extracts a minimum converted data volume and a maximum converted data volume from each converted data volume in a data volume set after conversion, where a range between the minimum converted data volume and the maximum converted data volume is the data volume range.

[0099] Correspondingly, the collecting, by the server, statistics on a target quantity of data volumes of each target segment in the plurality of target segments from the data volume set described in S3083 includes: collecting, by the server, statistics on a target quantity of converted data volumes of the each target segment in the plurality of target segments from the converted data volume set. In other words, the server determines the target segment of the each converted data volume in the converted data volume set, to further collect statistics on a quantity of the converted data volumes of the each target segment in the plurality of target segments. The quantity of the converted data volumes of the each target segment obtained by collecting statistics is the target quantity corresponding to the each target segment. In addition, the data volume such as the target data volume is a corresponding data volume after conversion.

[0100] In this embodiment of this application, S310 may be implemented through S3101 to S3105. In other words, the traversing, by the server, the first object set, and constructing at least one second object sub-model based on the first sub-model corresponding to the traversed first object includes S3101 to S3105. The steps are described as follows:
S3101: Traverse the first object set, determining a first sub-model corresponding to the 1st traversed first object as a current sub-model, and construct the 1st current sub-model set including the current sub-model.

[0101] When the first object set is traversed, a current sub-model set corresponding to an associated second object is an empty set in a case that the traversed first object is the 1st traversed first object. In this case, the server uses first sub-model corresponding to the 1st traversed first object as the current sub-model and an element in the current sub-model set, to construct the 1st current sub-model set.

[0102] S3102: Perform the following processing by iterating i: comparing a first sub-model corresponding to a traversed i^{th} first object with each current sub-model in an $(i-1)^{th}$ current sub-model set, to obtain a similar sub-model,$2 < i \leq I$, i being an incremental positive integer variable, and I being a quantity of first objects in the first object set.

[0103] In a case that the traversed first object is another first object traversed after the 1st traversed first object, the server compares a first sub-model corresponding to a traversed i^{th} first object with each current sub-model in an $(i-1)^{th}$ current sub-model set, and selects a current sub-model most similar to the first sub-model corresponding to the i^{th} first object from the $(i-1)^{th}$ current sub-model set according to a comparison result, so that the similar sub-model is obtained.

[0104] S3103: Merge the first sub-model corresponding to the i^{th} first object and the similar sub-model in a case that a similarity between the first sub-model corresponding to the i^{th} first object and the similar sub-model is greater than a first preset similarity, to obtain a merged sub-model, and replace the similar sub-model in the $(i-1)^{th}$ current sub-model set with the merged sub-model, to obtain an i^{th} current sub-model set.

[0105] After obtaining the similar sub-model, the server compares a similarity between the similar sub-model and the first sub-model corresponding to the i^{th} first object with the first preset similarity. In a case that the similarity between the similar sub-model and the first sub-model corresponding to the i^{th} first object is greater than the first preset similarity, it indicates that a first object (for example, a convenience store A) corresponding to the first sub-model corresponding to the i^{th} first object is similar to a first object (for example, convenience store B) corresponding to the similar sub-model in terms of the data volume. In this case, the server merges the first sub-model corresponding to the i^{th} first object and the similar sub-model, and a merged result is the merged sub-model. Then, the server replaces the similar sub-model in the $(i-1)^{th}$ current sub-model set with the merged sub-model, and the $(i-1)^{th}$ current sub-model set after replacement is the i^{th} current sub-model set.

[0106] S3104: Insert a to-be-updated sub-model into the current sub-model set in a case that the similarity between the first sub-model corresponding to the i^{th} first object and the similar sub-model is less than or equal to the first preset similarity, to update the current sub-model set.

[0107] In a case that the similarity between the similar sub-model and the first sub-model corresponding to the i^{th} first object is less than or equal to the first preset similarity, it indicates that a first object (for example, a convenience store A) corresponding to the first sub-model corresponding to the i^{th} first object is not similar to a first object (for example, convenience store B) corresponding to the similar sub-model in terms of the data volume. In this case, the server inserts the first sub-model corresponding to the i^{th} first object into the $(i-1)^{th}$ current sub-model set, and the $(i-1)^{th}$ current sub-model set after insertion is the i^{th} current sub-model set.

[0108] S3105: Determine an I^{th} current sub-model set obtained by iterating i as the at least one second object sub-model.

[0109] In this embodiment of this application, when the server traverses the first object set, for any first object in the first object set, a current sub-model set corresponding to a current first object is updated by performing S3102 to S3104. After the first object set is traversed, an obtained current sub-model set after traversal and update is the constructed at least one second object sub-model.

[0110] In this embodiment of this application, S3102 further includes S31021 to S31024. In other words, the comparing, by the server, a to-be-updated sub-model corresponding to the current first object in the first preset object model with each current sub-model in a current sub-model set corresponding to each second object, to obtain a similar sub-model includes S31021 to S31024. The steps are described as follows:

S31021: Obtain a plurality of first target probability values corresponding to the plurality of target segments from the first sub-model corresponding to the traversed i^{th} first object.

[0111] Since a first sub-model corresponding to each first object is a plurality of probability values corresponding to the plurality of target segments, the first sub-model corresponding to the traversed i^{th} first object also includes the plurality of probability values corresponding to the plurality of target segments, referred to as the first target probability values corresponding to the target segments herein. That is, the plurality of first target probability values corresponding to the plurality of target segments refer to a relationship between a plurality of target segments and a plurality of probability values corresponding to the to-be-updated sub-model. The plurality of target segments and the plurality of first target probability values are in a one-to-one correspondence.

[0112] S31022: Obtain a plurality of second target probability values corresponding to the plurality of target segments from the each current sub-model in the $(i-1)^{th}$ current sub-model set.

[0113] The each current sub-model in the $(i-1)^{th}$ current sub-model set also includes the plurality of probability values corresponding to the plurality of target segments, referred to as the plurality of second target probability values corresponding to the plurality of target segments herein. That is, the plurality of second target probability values corresponding to the plurality of target segments refer to a relationship between a plurality of target segments and a plurality of probability values corresponding to the each current sub-model. The plurality of target segments and the plurality of second target probability values are in a one-to-one correspondence.

[0114] S31023: Compare the plurality of first target probability values with the plurality of second target probability values one by one to obtain a plurality of minimum probability values, and determine an accumulated sum of the plurality of minimum probability values as a similarity between the first sub-model corresponding to the ith first object and the each current sub-model.

[0115] Since the plurality of first target probability values and the plurality of second target probability values are in a one-to-one correspondence, the server further compares a plurality of first target probability values of the first sub-model corresponding to the traversed ith first object with a plurality of second target probability values of the each current sub-model, to determine the similarity between the first sub-model corresponding to the traversed ith first object and the each current sub-model. At least one similarity corresponding to at least one current sub-model in the (i-1)th current sub-model set is obtained after the similarity between the first sub-model corresponding to the traversed ith first object and the each current sub-model is obtained.

[0116] The plurality of minimum probability values and the plurality of first target probability values are in a one-to-one correspondence, the plurality of minimum probability values and the plurality of second target probability values are in a one-to-one correspondence, and the at least one current sub-model in the (i-1)th current sub-model set and the plurality of similarities are in a one-to-one correspondence.

[0117] Referring to FIG. 7, FIG. 7 is an exemplary schematic diagram of obtaining a similarity according to an embodiment of this application. As shown in FIG. 7, in a coordinate system in which a horizontal coordinate is a logarithm-taking amount value and a vertical coordinate is a probability value, a similarity between a first sub-model 7-1 corresponding to the ith first object and each current sub-model 7-2 is an area corresponding to a region 7-3. In a case that a plurality of first target probability values corresponding to the first sub-model 7-1 corresponding to the ith first object is a_j, a plurality of second target probability values corresponding to the current sub-model 7-2 is b_j, and j is an integer greater than or equal to 2, a similarity S between the first sub-model 7-1 corresponding to the ith first object and the current sub-model 7-2 is shown in formula (1):

$$S = \sum_{j=1}^{n} min\,(a_j, b_j) \qquad (1),$$

where

n is a quantity of the plurality of target segments.

[0118] S31024: Select a highest similarity from determined at least one similarity corresponding to the (i-1)th current sub-model set, and determine a current sub-model corresponding to the highest similarity in the (i-1)th current sub-model set as the similar sub-model.

[0119] In this embodiment of this application, the server obtains the highest similarity from the plurality of similarities, and uses a current sub-model corresponding to the highest similarity in the (i-1)th current sub-model set as the similar sub-model.

[0120] In this embodiment of this application, the merging, by the server, the first sub-model corresponding to the ith first object and the similar sub-model, to obtain a merged sub-model described in S3103 includes S31031 to S31034. The steps are described as follows:

[0121] S31031: Obtain a plurality of first target probability values corresponding to the plurality of target segments from the first sub-model corresponding to the ith first object.

[0122] An implementation process of S31031 is consistent with the implementation process described in S31021.

[0123] S31032: Obtain a plurality of to-be-merged probability values corresponding to the plurality of target segments from the similar sub-model.

[0124] The each current sub-model also includes the plurality of probability values corresponding to the plurality of target segments, referred to as the plurality of second target probability values corresponding to the plurality of target segments herein. That is, the plurality of second target probability values corresponding to the plurality of target segments refer to a relationship between a plurality of target segments and a plurality of probability values corresponding to the each current sub-model, where the plurality of target segments and the plurality of to-be-merged probability values.

[0125] S31033: Compare the plurality of first target probability values with the plurality of to-be-merged probability values one by one, to obtain a plurality of maximum probability values.

[0126] The plurality of first target probability values and the plurality of to-be-merged probability values are in a one-to-one correspondence, the plurality of maximum probability values and the plurality of first target probability values are in a one-to-one correspondence, and the plurality of maximum probability values and the plurality of to-be-merged probability values are in a one-to-one correspondence.

[0127] S31034: Combine the plurality of target segments and the plurality of maximum probability values, to obtain the merged sub-model.

[0128] Referring to FIG. 8, FIG. 8 is an exemplary schematic diagram of obtaining a merged sub-model according to an embodiment of this application. As shown in FIG. 8, in a coordinate system in which a horizontal coordinate is a logarithm-taking amount value and a vertical coordinate is a probability value, a first sub-model 8-1 corresponding to the i^{th} first object and a merged sub-model 8-3 corresponding to a similar sub-model 8-2 are shown. In a case that a plurality of first target probability values corresponding to the first sub-model 8-1 corresponding to the i^{th} first object is a_j, and a plurality of to-be-merged probability values corresponding to the similar sub-model 8-2 is c_j, a process in which the first sub-model 8-1 corresponding to the i^{th} first object and the similar sub-model 8-2 are merged to obtain the merged sub-model 8-3 may be implemented by using formula (2), which is expressed as follows:

$$C = \{\ldots, \max(a_j, c_j), \ldots\}, \mathrm{i} \in \mathrm{n} \qquad (2),$$

, where
C is used for representing the merged sub-model 8-3.

[0129] In this embodiment of this application, S304 may be implemented through S3041 to S3044. In other words, the obtaining, by the server, a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model includes S3041 to S3044. The steps are described as follows:
S3041: Obtain at least one target second object sub-model corresponding to the second target object from the second preset object model.

[0130] Since the second object sub-model is obtained by combining at least one second preset object model corresponding to each second object, the server matches the second target object with the each second object in the second preset object model, and at least one second object sub-model corresponding to a matched second object is the at least one target second object sub-model.

[0131] S3042: Obtain at least one target similarity between the first target sub-model and the at least one target second object sub-model.

[0132] In this embodiment of this application, the server compares the first target sub-model with each target second object sub-model, so that a target similarity between the first target sub-model and the each target second object sub-model is obtained, and the at least one target similarity corresponding to the at least one target second object sub-model is obtained. The at least one target second object sub-model and the at least one target similarity are in a one-to-one correspondence.

[0133] A process of obtaining a plurality of target similarities by the server is similar to the processes of obtaining a plurality of similarities described in S31011 to S31013. Details are not described again in this embodiment of this application.

[0134] S3043: Obtain a highest target similarity from the at least one target similarity.

[0135] The highest target similarity is a target similarity that is highest in the at least one target similarity corresponding to the at least one target second object sub-model.

[0136] S3044: Determine a target second object sub-model corresponding to the highest target similarity in the at least one target second object sub-model as the second target sub-model.

[0137] The server selects a corresponding target second object sub-model from the at least one target second object sub-model according to the highest target similarity, and determines the selected target second object sub-model corresponding to the highest target similarity as the second target sub-model. The second target sub-model has the highest similarity with the first target sub-model.

[0138] In this embodiment of this application, the obtaining, by the server, a target maximum data volume corresponding to the second target sub-model described in S305 includes: determining, by the server, a maximum data volume corresponding to the second target object in the second preset object model as the target maximum data volume corresponding to the second target sub-model in a case that the highest target similarity is greater than a second preset similarity; and determining, by the server, a preset data volume as the target maximum data volume corresponding to the second target sub-model in a case that the highest target similarity is less than or equal to the second preset similarity. The preset data volume may be, for example, 0 or any other value. In addition, the first preset similarity and the second preset similarity may be the same or different. This is not specifically limited in this embodiment of this application.

[0139] The following describes an exemplary application of this embodiment of this application in an actual application scenario by using an example in which abnormality detection is performed on a payment order in a payment scenario of an instant messaging client.

[0140] Referring to FIG. 9, FIG. 9 is an exemplary schematic flowchart of abnormal behavior detection according to an embodiment of this application. As shown in FIG. 9, in a payment scenario, after a user submits a payment order 9-1 (to-be-detected behavior information), first, before the payment is completed according to the payment order, the server pulls the payment order and obtains an order triplet 9-2 from the payment order: a user 9-21 (a first target object), a merchant 9-22 (a first target object), and an amount value 9-23 (a target data volume).

[0141] Then, the server obtains a merchant histogram 9-311 (a first target sub-model) corresponding to the merchant 9-22 from a merchant model 9-31 (a first preset object model), and determines a normal transaction threshold t_u (an abnormal data volume) of the merchant 9-22 according to a 99th quantile (a preset model parameter) of the merchant histogram 9-311; The process of determining the normal transaction threshold t_u, is shown in FIG. 4. It is easy to learn that, the normal transaction threshold t_u indicates that, in a case that an amount value is greater than the normal transaction threshold t_u, a payment order corresponding to the amount value exceeds 99% of the normal situation, and it is determined that the payment order corresponding to the amount value is an abnormal transaction on a merchant side. Since the amount value 9-23 is greater than the normal transaction threshold t_u, it indicates that the payment order 9-1 exceeds 99% of the normal situation, and it is determined that the payment order 9-1 is of a result 9-41 (a first detection result) of abnormal transaction on the merchant side.

[0142] Then, the server obtains a merchant histogram group 9-321 (at least one target second object sub-model) corresponding to the user 9-21 from a user model 9-32 (a second preset object model), and searches the merchant histogram group 9-321 for a merchant histogram 9-322 (a second target sub-model) most similar to the merchant histogram 9-311. In a case that a similarity between the merchant histogram 9-322 and the merchant histogram group 9-321 is greater than 0.8 (a second preset similarity), a historical maximum transaction amount (a maximum data volume corresponding to a second target object) corresponding to the user 9-21 in the user model 9-32 is obtained as the normal transaction t_v (a target maximum data volume). Otherwise, it indicates that the user 9-21 has not consumed at the merchant 9-22, and the normal transaction threshold t_v is set to 0 (a preset data volume). It is easy to learn that, the normal transaction threshold t_v indicates that, in a case that an amount value is less than or equal to the normal transaction threshold t_v, it indicates that the amount value has the same amount value in a historical payment order, and it is determined that a payment order corresponding to the amount value is a normal transaction on a user side. Since the amount value 9-23 is greater than the normal transaction threshold t_v, it indicates that the amount value 9-23 has not appeared in the historical payment order, and it is determined that the payment order 9-1 is of a result 9-42 (a second detection result) of abnormal transaction on the user side.

[0143] Finally, the payment order 9-1 is determined to be abnormal (a target detection result) according to a decision matrix shown in Table 1 according to the result 9-41 and the result 9-42, which may be a transaction performed by a stolen account. In view of this, blocking processing 9-5 is performed on the payment order 9-1 to improve the network security.

Table 1

User side Merchant side	Abnormal	Normal
Abnormal	Abnormal payment	Suspected abnormal payment
Normal	Normal payment	Normal payment

[0144] It is easy to learn from the decision matrix shown in FIG. 1 that, the payment order is determined to be abnormal in a case that the merchant side indicates that the payment order is abnormal and the user side indicates that the payment order is also abnormal; the payment order is determined to be normal in a case that the merchant side indicates that the payment order is abnormal and the user side indicates that the payment order is normal; the payment order is determined to be a suspected abnormal payment in a case that the merchant side indicates that the payment order is normal and the user side indicates that the payment order is abnormal, where in this case, abnormality of the payment order is determined according to an actual situation, that is, the payment order may be considered as normal or abnormal according to the actual situation; and the payment order is determined to be normal in a case that the merchant side indicates that the payment order is normal and the user side also indicates that the payment order is normal.

[0145] In addition, an embodiment of this application further provides another decision matrix, which is shown in Table 2:

Table 2

User side \ Merchant side	Abnormal	Normal
Abnormal	Abnormal payment	Suspected abnormal payment
Normal	Suspected abnormal payment	Normal payment

[0146] It is easy to learn from the decision matrix shown in FIG. 2 that, the payment order is determined to be abnormal in a case that the merchant side indicates that the payment order is abnormal and the user side indicates that the payment order is also abnormal; the payment order is determined to be a suspected abnormal payment in a case that the merchant side indicates that the payment order is abnormal and the user side indicates that the payment order is normal, where in this case, abnormality of the payment order is determined according to an actual situation, that is, the payment order may be considered as normal or abnormal according to the actual situation; the payment order is determined to be a suspected abnormal payment in a case that the merchant side indicates that the payment order is normal and the user side indicates that the payment order is abnormal, where in this case, abnormality of the payment order is determined according to an actual situation, that is, the payment order may be considered as normal or abnormal according to the actual situation; and the payment order is determined to be normal in a case that the merchant side indicates that the payment order is normal and the user side also indicates that the payment order is normal.

[0147] There may be another decision matrix in a case that the server determines the target detection result according to the first detection result and the second detection result. This is not listed one by one in this embodiment of this application.

[0148] In addition, the foregoing process of determining the abnormality of the payment order is real-time, which is implemented in a real-time/online environment. The foregoing process of determining the abnormality of the payment order may further be applied to a scenario such as credit card anti-spoofing or black market confrontation.

[0149] It may be understood that, in the payment scenario of the instant messaging client, abnormality detection is performed, and processing such as payment blocking or authentication is performed in a case that the payment is determined to be abnormal based on a detection result, so that payment security of the instant messaging client can be ensured.

[0150] The following continues to describe the application of abnormal behavior detection in the payment scenario.

[0151] Referring to FIG. 10, FIG. 10 is an exemplary schematic diagram of obtaining a model according to an embodiment of this application. As shown in FIG. 10, the server obtains a historical payment order 10-1 (a behavior information sample) recently generated (in a current preset cycle), where each payment order in the historical payment order 10-1 includes a user (a second object), a merchant (a first object), and an amount (a data volume).

[0152] First, the historical payment order 10-1 is aggregated according to the merchant (a first preset object type) to obtain a transaction amount 10-2 (a data volume set) of all recent users of each merchant; after the transaction amount 10-2 of all the recent users of the each merchant is converted by using a natural logarithm, segmented statistics is collected, to obtain an amount distribution histogram 10-31 (a first sub-model), where a histogram 11-1 shown in FIG. 11 is the amount distribution histogram 10-31 in FIG. 10, and in a coordinate system, a horizontal coordinate is logarithm-taking amount value and a vertical coordinate is a probability value; and the amount distribution histogram 10-31 corresponding to the each merchant is combined, to obtain a merchant model 10-3.

[0153] Further, the historical payment order 10-1 is aggregated according to the user (a second preset object type) to obtain merchants 10-41 (a first object set) that each user has recently paid for and a payment amount 10-42 of the each user recently paid for the merchants, and selects a maximum payment amount 10-421 (a maximum data volume) from the payment amount 10-42 of the each user recently paid for the merchants as a historical maximum payment amount.

[0154] Then, the merchants 10-41 that each user has recently paid for are traversed, a corresponding merchant amount distribution histogram 10-32 is obtained from the merchant model 10-3 for each merchant 10-411 (an i^{th} first object). The merchant amount distribution histogram 10-32 is directly inserted into a histogram group 10-51 (a current sub-model set) in a case that each merchant 10-411 is the first traversed merchant in the merchants 10-41; and the merchant amount distribution histogram 10-32 is compared with each histogram in the histogram group 10-51 in a case that each merchant 10-411 is not the first traversed merchant in the merchants 10-41, to compare a histogram 10-511 (a similar sub-model) with the highest similarity from the histogram group 10-51. The comparison process is shown in FIG. 7. The merchant amount distribution histogram 10-32 is merged into the histogram 10-511 in a case that a similarity between the histogram 10-511 and the merchant amount distribution histogram 10-32 is greater than 0.8 (a first preset similarity), where the merging process is shown in FIG. 8; and the merchant amount distribution histogram 10-32 is inserted into the histogram group 10-51 in a case that the similarity between the histogram 10-511 and the merchant amount distribution histogram 10-32 is less than or equal to 0.8. In this way, after the merchants 10-41 are traversed (where the histogram group 10-51 is at least one second object sub-model), the histogram group 10-51 corresponding to each user is combined with the maximum payment amount 10-421 to obtain the second sub-model, so that a user model 10-5 (a second preset object model) is obtained.

[0155] The process of obtaining the first preset object model and the second preset object model may be performed in an offline environment.

[0156] It may be understood that, the abnormal behavior detection method provided in the embodiments of this application is performed in an unsupervised manner, and there is no need to label, thereby improving the enforceability of detection in the payment scenario of the instant messaging client. Furthermore, in the process of obtaining the merchant model and the user model, only the merchant, the user, and the amount value are required, so that abnormal behavior detection in the payment scenario of the instant messaging client may be accurately implemented even in a case that there are three dimensional features. In addition, since data annotation is not required for obtaining the merchant model and the user model, the obtaining efficiency is improved, so that the obtained merchant model and the user model are time-based and can be applied to a real-time payment environment of the instant messaging client.

[0157] The following further describes an exemplary structure in which the abnormal behavior detection apparatus 455 provided in this embodiment of this application is implemented as software modules. In some embodiments, as shown in FIG. 2, the software module stored in the abnormal behavior detection apparatus 455 of the memory 450 may include:

an information obtaining module 4551, configured to obtain to-be-detected behavior information, the to-be-detected behavior information including a first target object, a second target object, and a target data volume;

a first detection module 4552, configured to obtain a first target sub-model corresponding to the first target object from a first preset object model,

the first detection module 4552 being further configured to determine an abnormal data volume from the first target sub-model based on a preset model parameter, and determine a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume;

a second detection module 4553, configured to obtain a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model,

the second detection module 4553 being further configured to obtain a target maximum data volume corresponding to the second target sub-model, and determine a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume; and

a result determination module 4554, configured to determine a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result.

[0158] In this embodiment of this application, the abnormal behavior detection apparatus 455 further includes a model obtaining module 4555, configured to: obtain a behavior information sample; aggregate the behavior information sample according to a first preset object type to obtain a data volume set corresponding to each first object, construct a first sub-model corresponding to the each first object according to the data volume set, and determine each constructed first sub-model corresponding to the each first object as the first preset object model; aggregate the behavior information sample according to a second preset object type, to obtain a first object set and a maximum data volume corresponding to each second object; traverse the first object set, and constructing at least one second object sub-model based on the first sub-model corresponding to the traversed first object; and combine the at least one second object sub-model and the maximum data volume into a second sub-model corresponding to the each second object, and determine each combined second sub-model corresponding to the each second object as the second preset object model.

[0159] In this embodiment of this application, the model obtaining module 4555 is further configured to: obtain a data volume range corresponding to each data volume in the data volume set; segment the data volume range to obtain a plurality of target segments; collect statistics on a target quantity of data volumes of each target segment in the plurality of target segments from the data volume set; determine a ratio of the target quantity to a set element quantity corresponding to the data volume set as a probability value corresponding to the each target segment; and determine a plurality of determined probability values corresponding to the plurality of target segments as the first sub-model corresponding to the each first object.

[0160] In this embodiment of this application, the model obtaining module 4555 is further configured to: convert the each data volume in the data volume set, to obtain a converted data volume set; and determine a range corresponding to each converted data volume in the converted data volume set as the data volume range.

[0161] In this embodiment of this application, the model obtaining module 4555 is further configured to collect statistics on a target quantity of converted data volumes of the each target segment in the plurality of target segments from the converted data volume set.

[0162] In this embodiment of this application, the model obtaining module 4555 is further configured to: traverse the first object set, determine a first sub-model corresponding to the 1st traversed first object as a current sub-model, and construct the 1st current sub-model set including the current sub-model; and perform the following processing by iterating i: comparing a first sub-model corresponding to a traversed i^{th} first object with each current sub-model in an $(i-1)^{th}$ current sub-model set, to obtain a similar sub-model,$2 < i \leq I$, i being an incremental positive integer variable, and I being a quantity of first objects in the first object set; merge the first sub-model corresponding to the i^{th} first object and the similar sub-model in a case that a similarity between the first sub-model corresponding to the i^{th} first object and the similar sub-model is greater than a first preset similarity, to obtain a merged sub-model, and replace the similar sub-model in the $(i-1)^{th}$ current sub-model set with the merged sub-model, to obtain an i^{th} current sub-model set; insert the first sub-model corresponding to the i^{th} first object into the $(i-1)^{th}$ current sub-model set in a case that the similarity between the first sub-model corresponding to the i^{th} first object and the similar sub-model is less than or equal to the first preset similarity, to obtain the i^{th} current sub-model set; and determine an I^{th} current sub-model set obtained by iterating i as the at least one second object sub-model.

[0163] In this embodiment of this application, the model obtaining module 4555 is further configured to: obtain a plurality of first target probability values corresponding to the plurality of target segments from the first sub-model corresponding to the traversed i^{th} first object; obtain a plurality of second target probability values corresponding to the plurality of target segments from the each current sub-model in the $(i-1)^{th}$ current sub-model set; compare the plurality of first target probability values with the plurality of second target probability values one by one to obtain a plurality of minimum probability values, and determine an accumulated sum of the plurality of minimum probability values as a similarity between the first sub-model corresponding to the i^{th} first object and the each current sub-model; and select a highest similarity from determined at least one similarity corresponding to the $(i-1)^{th}$ current sub-model set, and determine a current sub-model corresponding to the highest similarity in the $(i-1)^{th}$ current sub-model set as the similar sub-model.

[0164] In this embodiment of this application, the model obtaining module 4555 is further configured to: obtain a plurality of first target probability values corresponding to the plurality of target segments from the first sub-model corresponding to the i^{th} first object; obtain a plurality of to-be-merged probability values corresponding to the plurality of target segments from the similar sub-model; compare the plurality of first target probability values with the plurality of to-be-merged probability values one by one, to obtain a plurality of maximum probability values; and combine the plurality of target segments and the plurality of maximum probability values, to obtain the merged sub-model.

[0165] In this embodiment of this application, the second detection module 4553 is further configured to: obtain at least one target second object sub-model corresponding to the second target object from the second preset object model; obtain at least one target similarity between the first target sub-model and the at least one target second object sub-model; obtain a highest target similarity from the at least one target similarity; and determine a target second object sub-model corresponding to the highest target similarity in the at least one target second object sub-model as the second target sub-model.

[0166] In this embodiment of this application, the second detection module 4553 is further configured to: determine a maximum data volume corresponding to the second target object in the second preset object model as the target maximum data volume corresponding to the second target sub-model in a case that the highest target similarity is greater than a second preset similarity; and determine a preset data volume as the target maximum data volume corresponding to the second target sub-model in a case that the highest target similarity is less than or equal to the second preset similarity.

[0167] In this embodiment of this application, the first detection module 4552 is further configured to: determine, in a case that the target data volume is greater than the abnormal data volume, that the to-be-detected behavior information is abnormal with respect to the first target object, the first detection result being that the to-be-detected behavior information is abnormal with respect to the first target object; and determine, in a case that the target data volume is less than or equal to the abnormal data volume, that the to-be-detected behavior information is normal with respect to the first target object, the first detection result being that the to-be-detected behavior information is normal with respect to the first target object.

[0168] In this embodiment of this application, the second detection module 4553 is further configured to: determine, in a case that the target data volume is greater than the target maximum data volume, that the to-be-detected behavior information is abnormal with respect to the second target object, the second detection result being that the to-be-detected behavior information is abnormal with respect to the second target object; and determine, in a case that the target data volume is less than or equal to the target maximum data volume, that the to-be-detected behavior information is normal with respect to the second target object, the second detection result being that the to-be-detected behavior information is normal with respect to the second target object.

[0169] In this embodiment of this application, the result determination module 4554 is further configured to: in a case that the first detection result is that the to-be-detected behavior information is abnormal with respect to the first target object and the second detection result is that the to-be-detected behavior information is abnormal with respect to the second target object, determine the target detection result including that the to-be-detected behavior information is abnormal; in a case that the first detection result is that the to-be-detected behavior information is normal with respect to the first target object and the second detection result is that the to-be-detected behavior information is abnormal with respect to the second target object, determine the target detection result including that the to-be-detected behavior information is abnormal; in a case that the first detection result is that the to-be-detected behavior information is normal with respect to the first target object and the second detection result is that the to-be-detected behavior information is normal with respect to the second target object, determine the target detection result including that the to-be-detected behavior information is normal; and in a case that the first detection result is that the to-be-detected behavior information is abnormal with respect to the first target object and the second detection result is that the to-be-detected behavior information is normal with respect to the second target object, determine the target detection result including that the to-be-detected behavior information is normal; and

[0170] An embodiment of this application provides a computer program product or a computer program. The computer program product or the computer program includes computer instructions, and the computer instructions are stored in a computer-readable storage medium. A processor of an abnormal behavior detection device reads the computer instructions from the computer-readable storage medium. The processor executes the computer instructions, to cause the computer device to perform the abnormal behavior detection method of the embodiments of this application.

[0171] An embodiment of this application provides a computer-readable storage medium storing executable instructions, the executable instructions, when executed by a processor, causing the processor to perform the abnormal behavior detection method provided in the embodiments of this application, for example, the abnormal behavior detection method shown in FIG. 3.

[0172] In some embodiments, the computer-readable storage medium may be a memory such as a ferroelectric RAM (FRAM), a ROM, a programmable ROM (PROM), an electrically programmable ROM (EPROM), an electrically erasable PROM (EEPROM), a flash memory, a magnetic surface memory, an optical disk, or a CD-ROM, or may be any device including one of or any combination of the foregoing memories.

[0173] In some embodiments, the executable instructions can be written in a form of a program, software, a software module, a script, or code and according to a programming language (including a compiler or interpreter language or a declarative or procedural language) in any form, and may be deployed in any form, including an independent program or a module, a component, a subroutine, or another unit suitable for use in a computing environment.

[0174] In an example, the executable instructions may, but do not necessarily, correspond to a file in a file system, and may be stored in a part of a file that saves another program or other data, for example, be stored in one or more scripts in a hypertext markup language (HTML) file, stored in a file that is specially used for a program in discussion, or stored in the plurality of collaborative files (for example, be stored in files of one or modules, subprograms, or code parts).

[0175] In an example, the executable instructions can be deployed for execution on one computing device, execution on a plurality of computing devices located at one location, or execution on a plurality of computing devices that are distributed at a plurality of locations and that are interconnected through a communication network.

[0176] Based on the above, in the embodiments of this application, in a case that the to-be-detected behavior information includes three dimensional features of the first target object, the second target object, and the target data volume, when the target detection result of whether the to-be-detected behavior information is abnormal is determined according to results of respectively comparing the target data volume with the abnormal data volume and the target maximum data volume, since the abnormal data volume is an abnormality judgment condition for the first target object determined based on the first preset object model, and the target maximum data volume is an abnormality judgment condition for the second target object determined based on the second preset object model, in a low-dimensional feature, whether the target data volume is within a preset interval is determined from two dimensions of the first target object and the second target object, to further accurately obtain the target detection result of whether the to-be-detected behavior information is abnormal, so that the accuracy of abnormal behavior detection is relatively high.

[0177] The foregoing descriptions are merely embodiments of this application and are not intended to limit the protection scope of this application. Any modification, equivalent replacement, or improvement made without departing from the spirit and range of this application shall fall within the protection scope of this application.

Claims

1. An abnormal behavior detection method, performed by an electronic device, the method comprising:

    obtaining to-be-detected behavior information, the to-be-detected behavior information comprising a first target object, a second target object, and a target data volume;
    obtaining a first target sub-model corresponding to the first target object from a first preset object model;
    determining an abnormal data volume from the first target sub-model based on a preset model parameter, and determining a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume;
    obtaining a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model;
    obtaining a target maximum data volume corresponding to the second target sub-model, and determining a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume; and
    determining a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result.

2. The method according to claim 1, wherein before the obtaining a first target sub-model corresponding to the first target object from a first preset object model, the method further comprises:

    obtaining a behavior information sample;
    aggregating the behavior information sample according to a first preset object type to obtain a data volume set corresponding to each first object, constructing a first sub-model corresponding to the each first object according to the data volume set, and determining each constructed first sub-model corresponding to the each first object as the first preset object model;
    aggregating the behavior information sample according to a second preset object type, to obtain a first object set and a maximum data volume corresponding to each second object;
    traversing the first object set, and constructing at least one second object sub-model based on the first sub-model corresponding to the traversed first object; and
    combining the at least one second object sub-model and the maximum data volume into a second sub-model corresponding to the each second object, and determining each combined second sub-model corresponding to the each second object as the second preset object model.

3. The method according to claim 2, wherein the constructing a first sub-model corresponding to the each first object according to the data volume set comprises:

    obtaining a data volume range corresponding to each data volume in the data volume set;
    segmenting the data volume range to obtain a plurality of target segments;
    collecting statistics on a target quantity of data volumes of each target segment in the plurality of target segments from the data volume set;
    determining a ratio of the target quantity to a set element quantity corresponding to the data volume set as a probability value corresponding to the each target segment; and
    determining a plurality of determined probability values corresponding to the plurality of target segments as the first sub-model corresponding to the each first object.

4. The method according to claim 3, wherein the obtaining a data volume range corresponding to each data volume in the data volume set comprises:

    converting the each data volume in the data volume set, to obtain a converted data volume set; and
    determining a range corresponding to each converted data volume in the converted data volume set as the data volume range; and
    the collecting statistics on a target quantity of data volumes of each target segment in the plurality of target segments from the data volume set comprises:
    collecting statistics on a target quantity of converted data volumes of the each target segment in the plurality of target segments from the converted data volume set.

5. The method according to any one of claims 2 to 4, wherein the traversing the first object set, and constructing at

least one second object sub-model based on the first sub-model corresponding to the traversed first object comprises:

traversing the first object set, determining a first sub-model corresponding to the 1st traversed first object as a current sub-model, and constructing the 1st current sub-model set comprising the current sub-model; and performing the following processing by iterating i:

comparing a first sub-model corresponding to a traversed i^{th} first object with each current sub-model in an $(i-1)^{th}$ current sub-model set, to obtain a similar sub-model,$2 < i \leq I$, i being an incremental positive integer variable, and I being a quantity of first objects in the first object set;
merging the first sub-model corresponding to the i^{th} first object and the similar sub-model in a case that a similarity between the first sub-model corresponding to the i^{th} first object and the similar sub-model is greater than a first preset similarity, to obtain a merged sub-model, and replacing the similar sub-model in the $(i-1)^{th}$ current sub-model set with the merged sub-model, to obtain an i^{th} current sub-model set;
inserting the first sub-model corresponding to the i^{th} first object into the $(i-1)^{th}$ current sub-model set in a case that the similarity between the first sub-model corresponding to the i^{th} first object and the similar sub-model is less than or equal to the first preset similarity, to obtain the i^{th} current sub-model set; and
determining an I^{th} current sub-model set obtained by iterating i as the at least one second object sub-model.

6. The method according to claim 5, wherein the comparing a first sub-model corresponding to a traversed i^{th} first object with each current sub-model in an $(i-1)^{th}$ current sub-model set, to obtain a similar sub-model comprises:

obtaining a plurality of first target probability values corresponding to the plurality of target segments from the first sub-model corresponding to the traversed i^{th} first object;
obtaining a plurality of second target probability values corresponding to the plurality of target segments from the each current sub-model in the $(i-1)^{th}$ current sub-model set;
comparing the plurality of first target probability values with the plurality of second target probability values one by one to obtain a plurality of minimum probability values, and determining an accumulated sum of the plurality of minimum probability values as a similarity between the first sub-model corresponding to the i^{th} first object and the each current sub-model; and
selecting a highest similarity from determined at least one similarity corresponding to the $(i-1)^{th}$ current sub-model set, and determining a current sub-model corresponding to the highest similarity in the $(i-1)^{th}$ current sub-model set as the similar sub-model.

7. The method according to claim 5, wherein the merging the first sub-model corresponding to the i^{th} first object and the similar sub-model, to obtain a merged sub-model comprises:

obtaining a plurality of first target probability values corresponding to the plurality of target segments from the first sub-model corresponding to the i^{th} first object;
obtaining a plurality of to-be-merged probability values corresponding to the plurality of target segments from the similar sub-model;
comparing the plurality of first target probability values with the plurality of to-be-merged probability values one by one, to obtain a plurality of maximum probability values; and
combining the plurality of target segments and the plurality of maximum probability values, to obtain the merged sub-model.

8. The method according to any one of claims 1 to 4, wherein the obtaining a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model comprises:

obtaining at least one target second object sub-model corresponding to the second target object from the second preset object model;
obtaining at least one target similarity between the first target sub-model and the at least one target second object sub-model;
obtaining a highest target similarity from the at least one target similarity; and
determining a target second object sub-model corresponding to the highest target similarity in the at least one target second object sub-model as the second target sub-model.

9. The method according to claim 8, wherein the obtaining a target maximum data volume corresponding to the second target sub-model comprises:

determining a maximum data volume corresponding to the second target object in the second preset object model as the target maximum data volume corresponding to the second target sub-model in a case that the highest target similarity is greater than a second preset similarity; and
determining a preset data volume as the target maximum data volume corresponding to the second target sub-model in a case that the highest target similarity is less than or equal to the second preset similarity.

10. The method according to any one of claims 1 to 4, wherein the determining a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume comprises:

determining, in a case that the target data volume is greater than the abnormal data volume, that the to-be-detected behavior information is abnormal with respect to the first target object, the first detection result being that the to-be-detected behavior information is abnormal with respect to the first target object; and
determining, in a case that the target data volume is less than or equal to the abnormal data volume, that the to-be-detected behavior information is normal with respect to the first target object, the first detection result being that the to-be-detected behavior information is normal with respect to the first target object.

11. The method according to any one of claims 1 to 4, wherein the determining a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume comprises:

determining, in a case that the target data volume is greater than the target maximum data volume, that the to-be-detected behavior information is abnormal with respect to the second target object, the second detection result being that the to-be-detected behavior information is abnormal with respect to the second target object; and
determining, in a case that the target data volume is less than or equal to the target maximum data volume, that the to-be-detected behavior information is normal with respect to the second target object, the second detection result being that the to-be-detected behavior information is normal with respect to the second target object.

12. The method according to any one of claims 1 to 4, wherein the determining a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result comprises:

in a case that the first detection result is that the to-be-detected behavior information is abnormal with respect to the first target object and the second detection result is that the to-be-detected behavior information is abnormal with respect to the second target object, determining the target detection result comprising that the to-be-detected behavior information is abnormal;
in a case that the first detection result is that the to-be-detected behavior information is normal with respect to the first target object and the second detection result is that the to-be-detected behavior information is abnormal with respect to the second target object, determining the target detection result comprising that the to-be-detected behavior information is abnormal;
in a case that the first detection result is that the to-be-detected behavior information is normal with respect to the first target object and the second detection result is that the to-be-detected behavior information is normal with respect to the second target object, determining the target detection result comprising that the to-be-detected behavior information is normal; and
in a case that the first detection result is that the to-be-detected behavior information is abnormal with respect to the first target object and the second detection result is that the to-be-detected behavior information is normal with respect to the second target object, determining the target detection result comprising that the to-be-detected behavior information is normal; and

13. An abnormal behavior detection apparatus, comprising:

an information obtaining module, configured to obtain to-be-detected behavior information, the to-be-detected behavior information comprising a first target object, a second target object, and a target data volume;
a first detection module, configured to obtain a first target sub-model corresponding to the first target object from a first preset object model,
the first detection module being further configured to determine an abnormal data volume from the first target

sub-model based on a preset model parameter, and determine a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume;

a second detection module, configured to obtain a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model,

the second detection module being further configured to obtain a target maximum data volume corresponding to the second target sub-model, and determine a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume; and

a result determination module, configured to determine a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result.

14. An abnormal behavior detection device, comprising:

a memory, configured to store executable instructions; and

a processor, configured to implement, when executing the executable instructions stored in the memory, the abnormal behavior detection method according to any one of claims 1 to 12.

15. A computer-readable storage medium, storing executable instructions, the instructions, when executed by a processor, implementing the abnormal behavior detection method according to any one of claims 1 to 12.

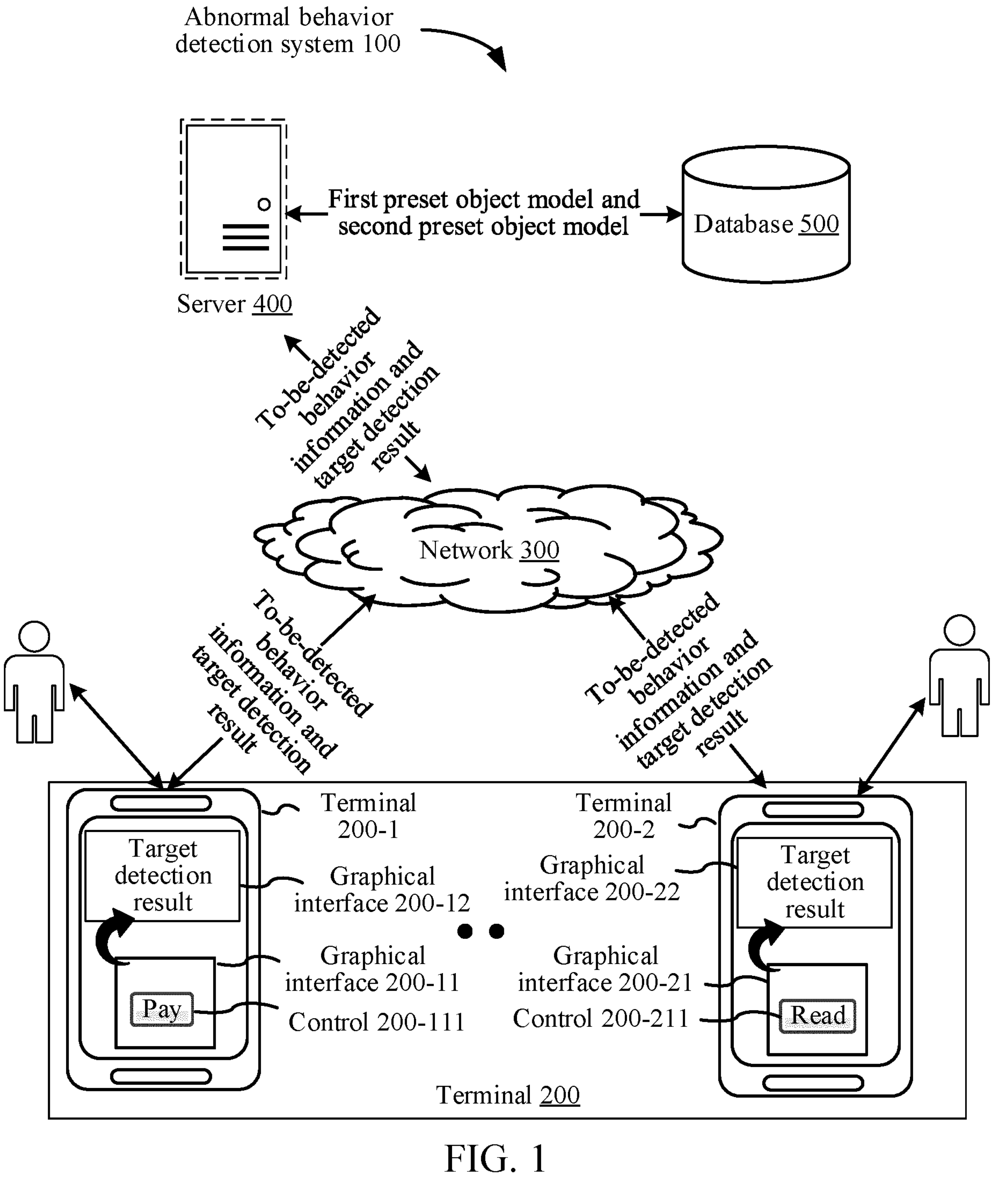

Abnormal behavior detection system 100
First preset object model and second preset object model
Database 500
Server 400
To-be-detected behavior information and target detection result
Network 300
To-be-detected behavior information and target detection result
To-be-detected behavior information and target detection result
Terminal 200-1
Target detection result
Graphical interface 200-12
Graphical interface 200-11
Pay
Control 200-111
Terminal 200-2
Graphical interface 200-22
Target detection result
Graphical interface 200-21
Control 200-211
Read
Terminal 200

FIG. 1

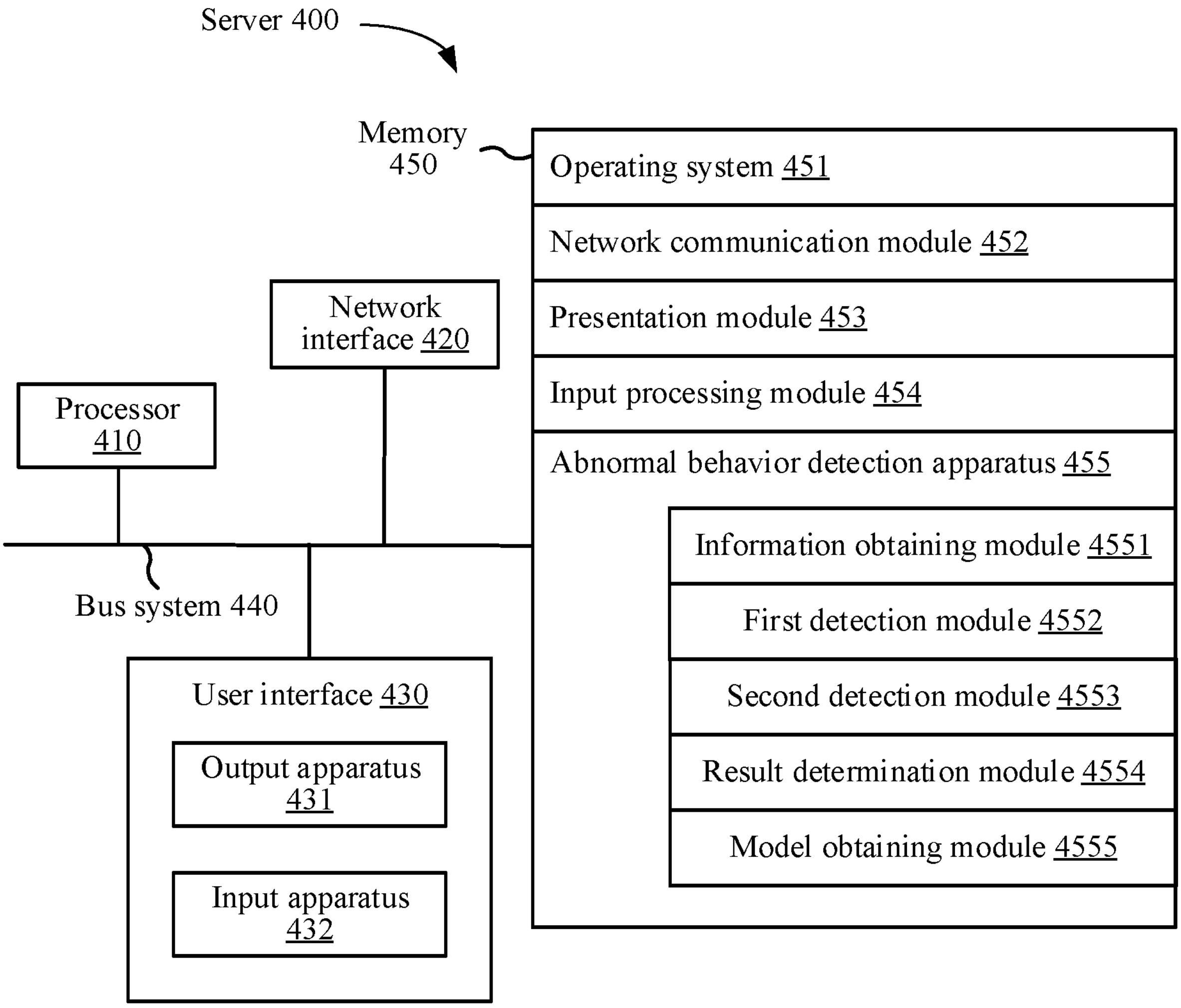
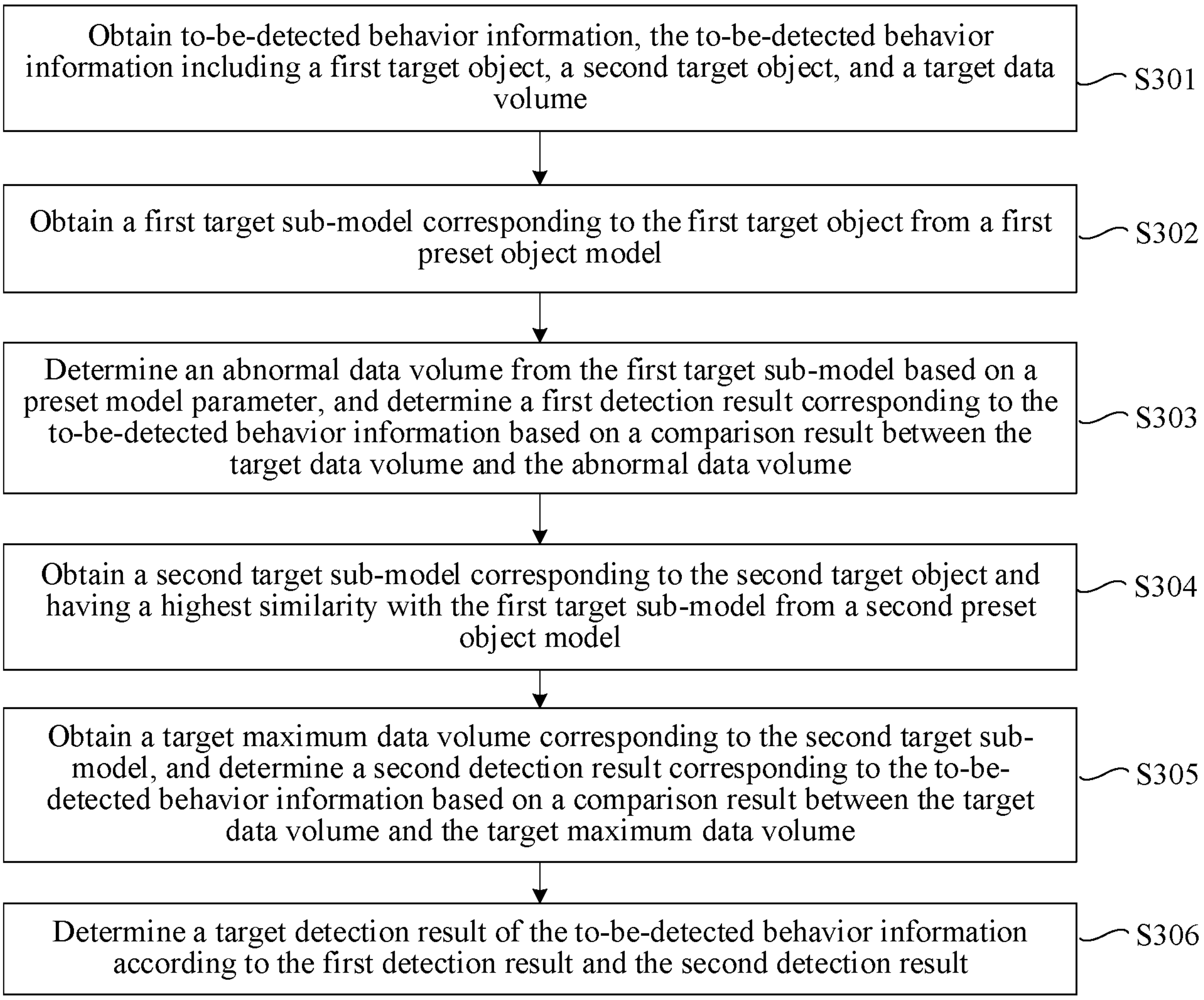

Server 400
Memory 450
Operating system 451
Network communication module 452
Presentation module 453
Input processing module 454
Abnormal behavior detection apparatus 455
Information obtaining module 4551
First detection module 4552
Second detection module 4553
Result determination module 4554
Model obtaining module 4555
Network interface 420
Processor 410
Bus system 440
User interface 430
Output apparatus 431
Input apparatus 432

FIG. 2



Obtain to-be-detected behavior information, the to-be-detected behavior information including a first target object, a second target object, and a target data volume S301

Obtain a first target sub-model corresponding to the first target object from a first preset object model S302

Determine an abnormal data volume from the first target sub-model based on a preset model parameter, and determine a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume S303

Obtain a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from a second preset object model S304

Obtain a target maximum data volume corresponding to the second target sub-model, and determine a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume S305

Determine a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result S306

FIG. 3

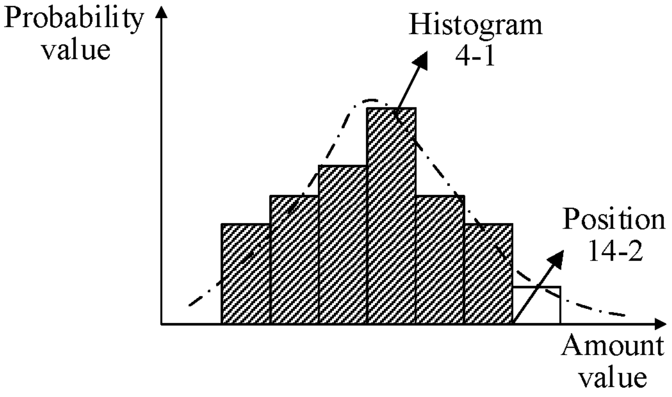


FIG. 4

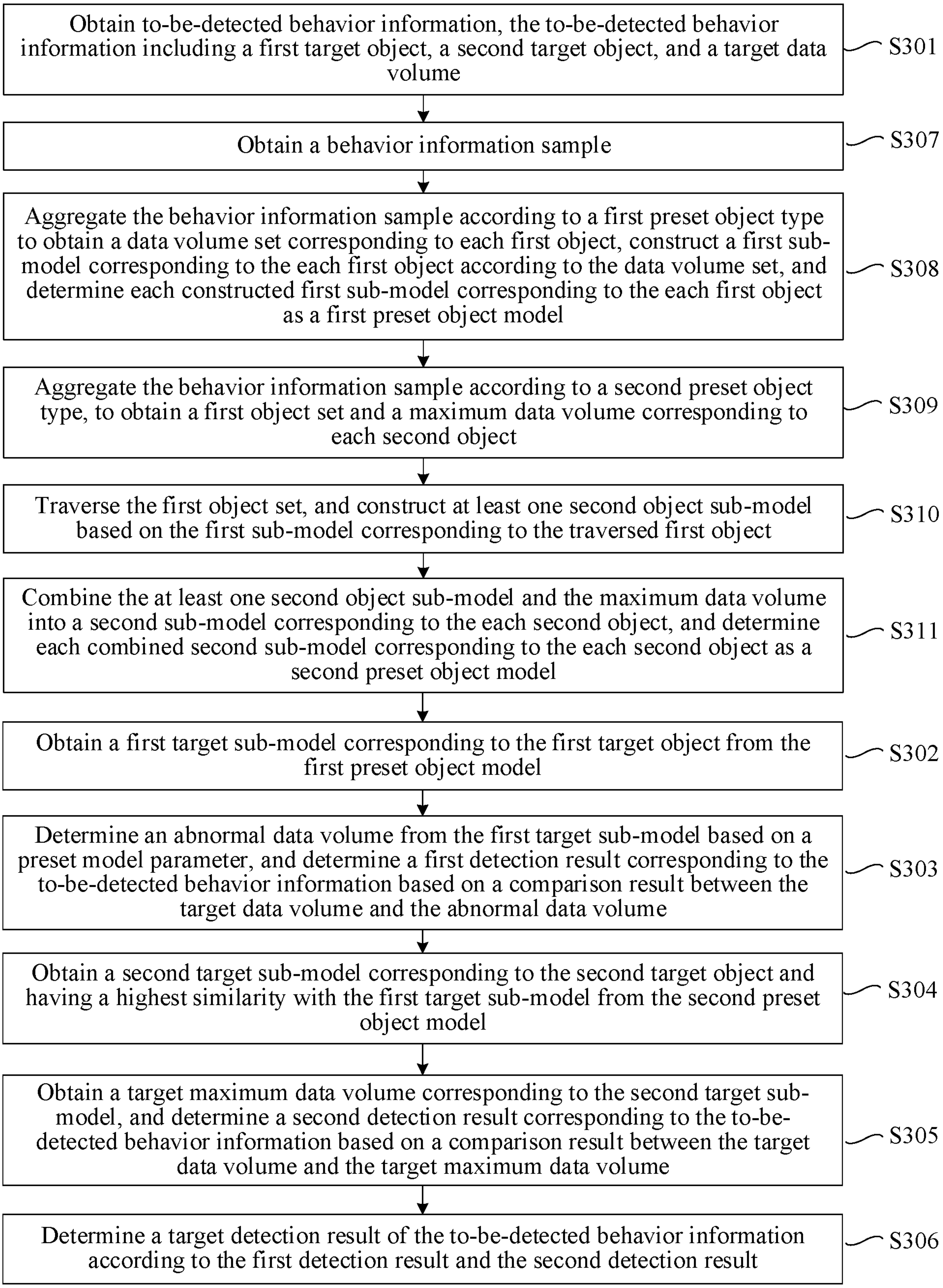

Obtain to-be-detected behavior information, the to-be-detected behavior information including a first target object, a second target object, and a target data volume
S301
Obtain a behavior information sample
S307
Aggregate the behavior information sample according to a first preset object type to obtain a data volume set corresponding to each first object, construct a first sub-model corresponding to the each first object according to the data volume set, and determine each constructed first sub-model corresponding to the each first object as a first preset object model
S308
Aggregate the behavior information sample according to a second preset object type, to obtain a first object set and a maximum data volume corresponding to each second object
S309
Traverse the first object set, and construct at least one second object sub-model based on the first sub-model corresponding to the traversed first object
S310
Combine the at least one second object sub-model and the maximum data volume into a second sub-model corresponding to the each second object, and determine each combined second sub-model corresponding to the each second object as a second preset object model
S311
Obtain a first target sub-model corresponding to the first target object from the first preset object model
S302
Determine an abnormal data volume from the first target sub-model based on a preset model parameter, and determine a first detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the abnormal data volume
S303
Obtain a second target sub-model corresponding to the second target object and having a highest similarity with the first target sub-model from the second preset object model
S304
Obtain a target maximum data volume corresponding to the second target sub-model, and determine a second detection result corresponding to the to-be-detected behavior information based on a comparison result between the target data volume and the target maximum data volume
S305
Determine a target detection result of the to-be-detected behavior information according to the first detection result and the second detection result
S306

FIG. 5

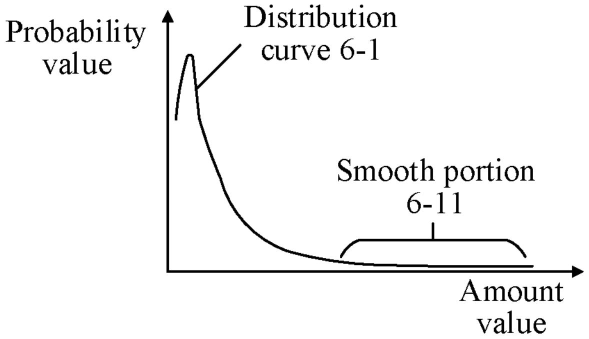


FIG. 6a

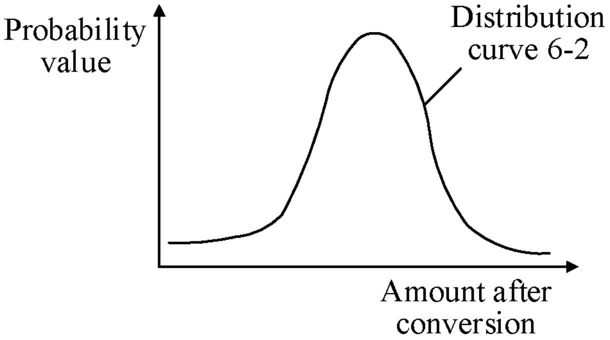


FIG. 6b

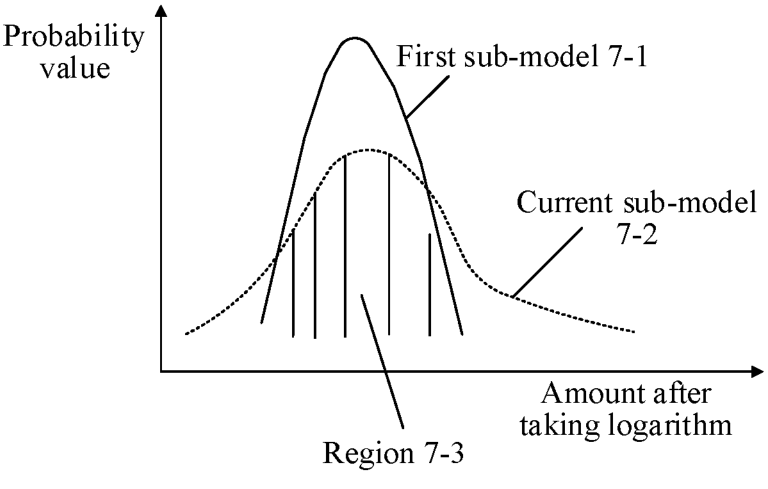


FIG. 7

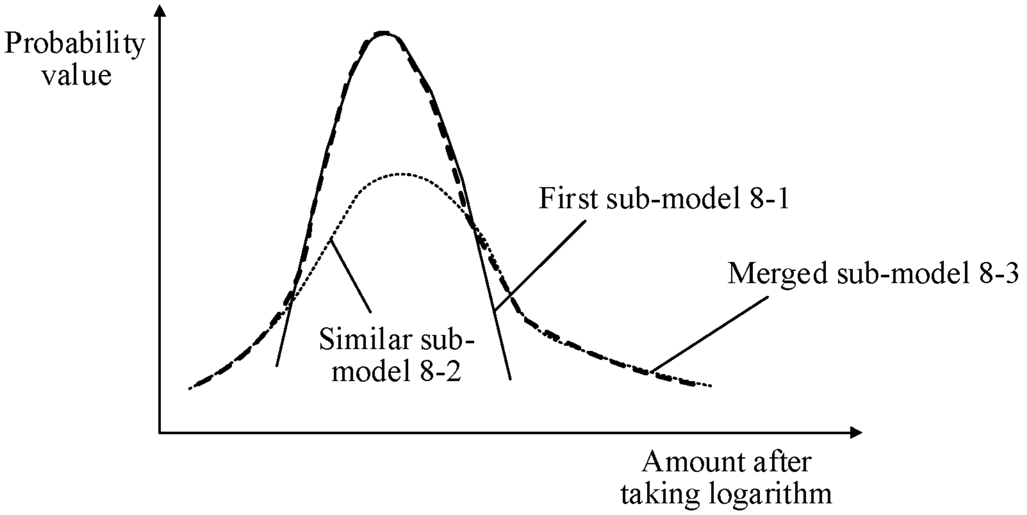

Probability value
First sub-model 8-1
Merged sub-model 8-3
Similar sub-model 8-2
Amount after taking logarithm

FIG. 8

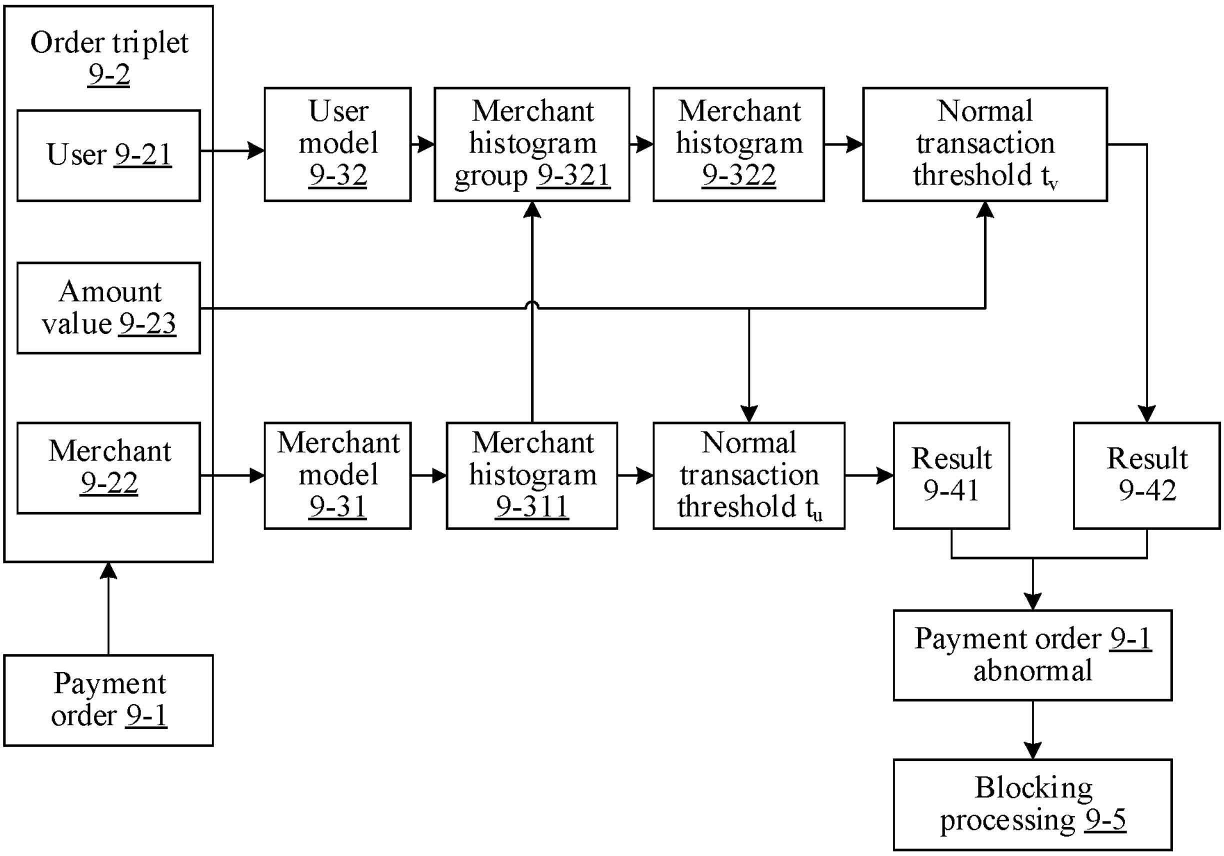

Order triplet 9-2
User 9-21
Amount value 9-23
Merchant 9-22
Payment order 9-1
User model 9-32
Merchant histogram group 9-321
Merchant histogram 9-322
Normal transaction threshold t_v
Merchant model 9-31
Merchant histogram 9-311
Normal transaction threshold t_u
Result 9-41
Result 9-42
Payment order 9-1 abnormal
Blocking processing 9-5

FIG. 9

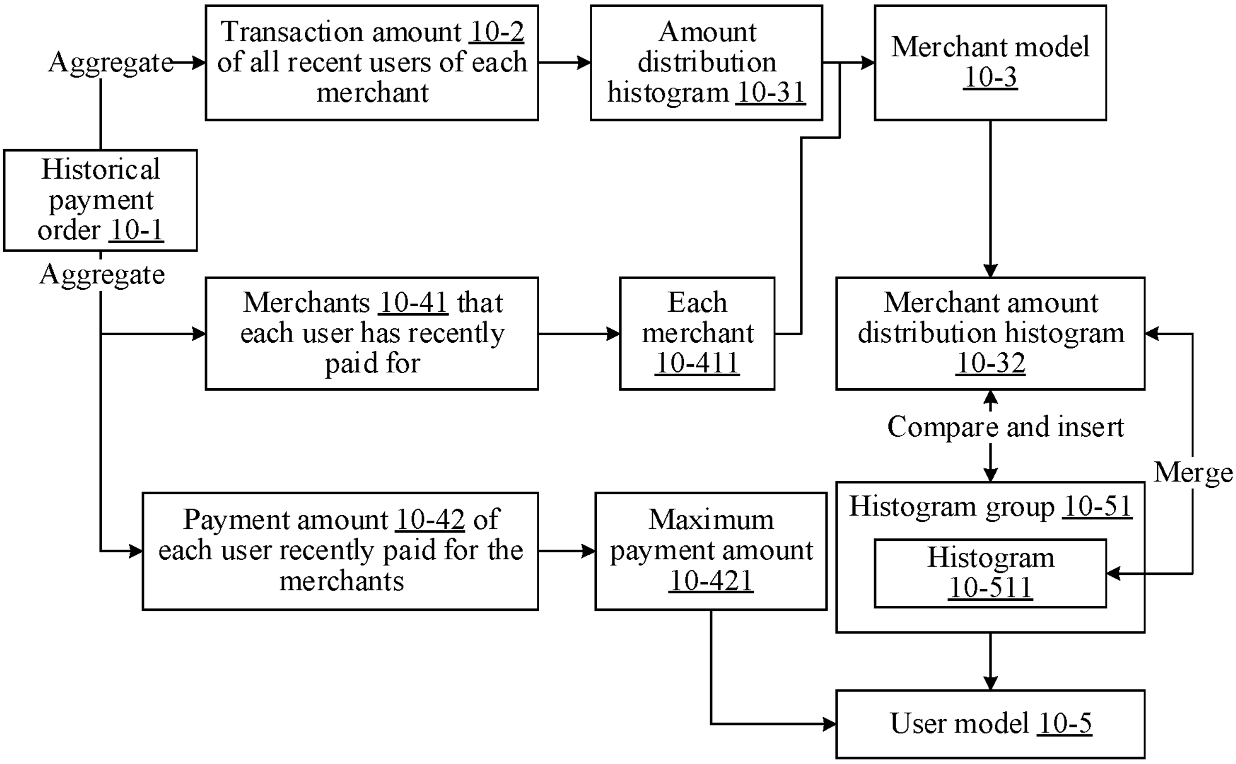

Aggregate
Transaction amount 10-2 of all recent users of each merchant
Amount distribution histogram 10-31
Merchant model 10-3
Historical payment order 10-1
Aggregate
Merchants 10-41 that each user has recently paid for
Each merchant 10-411
Merchant amount distribution histogram 10-32
Compare and insert
Merge
Payment amount 10-42 of each user recently paid for the merchants
Maximum payment amount 10-421
Histogram group 10-51
Histogram 10-511
User model 10-5

FIG. 10

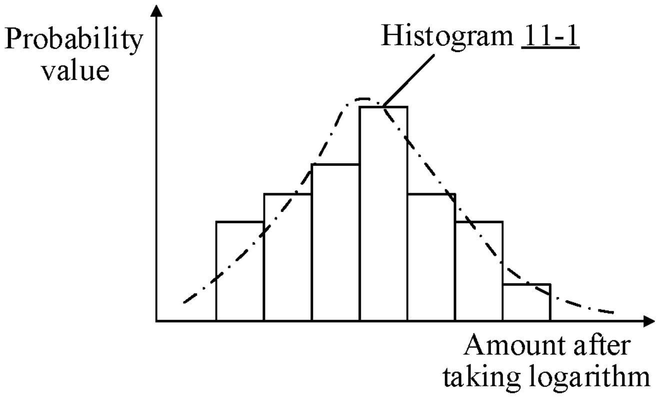

Probability value
Histogram 11-1
Amount after taking logarithm

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/104999

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q；G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; SIPOABS; DWPI; CNTXT; WOTXT; EPTXT; USTXT; CJFD; CNKI: 异常, 反常, 正常, 行为, 检测, 监测, 检查, 监视, 排查, 目标, 对象, 数据量, 模型, 参数, 对比, 比较, 相似度, 样本, 集, 聚合, 分段, 阈值, 概率, 比值, 浏览, 点击, 阅读, abnormal, unusual, anomaly, behavior, behaviour, pay, browse, click, view, watch, detect, monitor, examine, manage, object, amount, parameter, similarity, sample, set, cluster, threshold, probability, read

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103559420 A (SOOCHOW UNIVERSITY) 05 February 2014 (2014-02-05) entire document	1-15
A	CN 105843947 A (SOUTH CHINA NORMAL UNIVERSITY et al.) 10 August 2016 (2016-08-10) entire document	1-15
A	US 2020134504 A1 (ACER CYBER SECURITY INCORPORATED) 30 April 2020 (2020-04-30) entire document	1-15
A	US 2009210373 A1 (MATSUSHITA ELECTRIC IND. CO., LTD.) 20 August 2009 (2009-08-20) entire document	1-15

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search **05 October 2021**	Date of mailing of the international search report **13 October 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	Authorized officer
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/104999

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	103559420	A	05 February 2014	CN	103559420	B	28 September 2016
CN	105843947	A	10 August 2016	CN	105843947	B	05 March 2019
US	2020134504	A1	30 April 2020	TW	202016783	A	01 May 2020
				TW	I710922	B	21 November 2020
				EP	3648433	A1	06 May 2020
US	2009210373	A1	20 August 2009	WO	2009105299	A4	17 December 2009
				WO	2009105299	A3	15 October 2009
				WO	2009105299	A2	27 August 2009
				US	7962435	B2	14 June 2011

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader’s convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- CN 202010840924 **[0001]**